[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G10K 15/02
G06F 15/00 G06F 17/60
H04L 9/08 H04L 9/10
G06K 19/00 H04H 1/00
H04M 3/42 H04M 3/493
H04M 11/08 G10L 19/00
G06F 13/00 H04L 12/22

[12]发明专利申请公开说明书

[21]申请号 00814631.4

[43]公开日 2002年11月27日

[11]公开号 CN 1382292A

[22]申请日 2000.8.25 [21]申请号 00814631.4

[30]优先权

[32]1999.8.27 [33]JP [31]241747/99

[32]1999.12.3 [33]JP [31]345229/99

[86]国际申请 PCT/JP00/05770 2000.8.25

[87]国际公布 WO01/16932 日 2001.3.8

[85]进入国家阶段日期 2002.4.19

[71]申请人 富士通株式会社

地址 日本神奈川县川崎市

共同申请人 株式会社日立制作所

日本哥伦比亚株式会社

三洋电机株式会社

[72]发明人 畑中正行 蒲田顺 畠山卓久

长谷部高行 小谷诚刚 古田茂树

木下泰三 穴泽健明 日置敏昭

金森美和 堀吉宏

[74]专利代理机构 中国专利代理(香港)有限公司

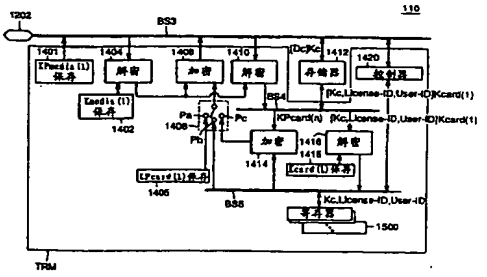
代理人 马铁良 叶恺东

权利要求书11页 说明书55页 附图56页

[54]发明名称 数据分发系统

[57]摘要

存储插件110通过解密处理从通过便携式电话网从服务器提供给数据总线BS3的数据中将对话Key Ks抽出。加密处理部1406根据对话Key Ks将存储插件110的公开加密密钥KPcard(1)加密并通过数据总线BS3提供给服务器。寄存器1500从服务器接受并存放所解密的许可ID、用户ID等数据,存储器1412从数据总线BS3接受并存放根据许可Key Kc所加密的加密内容数据[Dc]Kc。



ISSN1008-4274

1. 一种数据分发系统，用以从内容数据供给装置向复数用户的各终端分发加密内容数据，其中，

所述内容数据供给装置（10）具备:

第 1 接口部（350），用以在与外部之间交换数据;

第 1 对话 Key 发生部（314），生成在所述加密内容数据的每次通信时都被更新的第 1 公用密钥;

对话 Key 加密部（316），用以根据对应于所述用户的终端所预先确定的第 1 公开加密密钥将所述第 1 公用密钥加密并提供给所述第 1 接口部;

对话 Key 解密部（318），用以将根据所述第 1 公用密钥加密并回送的数据解密;

第 1 许可数据加密处理部（320），用以将由所述对话 Key 解密部所解密的数据作为密钥数据，对用于解密所述加密内容数据的许可 Key 进行加密;

第 2 许可数据加密处理部（322），用以将所述第 1 许可数据加密处理部的输出以第 2 公用密钥再行加密并提供给所述第 1 接口部进行分发，

各所述终端（100）具备:

第 2 接口部，用以在与外部之间交换数据;

分发数据解读部（110），接受并存放所述加密内容数据;

所述分发数据解读部具备:

第 1 密钥保存部（1402），保存用以解密根据所述第 1 公开加密密钥所加密的数据的第 1 秘密解密密钥;

第 1 解密处理部（1404），用以接受根据所述第 1 公开加密密钥所加密的所述第 1 公用密钥并进行解密处理;

第 2 密钥保存部（1405），用以保存第 2 公开加密密钥;

第 1 加密处理部（1406），用以根据所述第 1 公用密钥将所述第 2 公开加密密钥加密并向所述第 2 接口部输出;

第 2 解密处理部（1410），用以接受来自所述第 2 许可数据加密处理部的已加密的许可 Key 并根据所述第 2 公用密钥进行解密;

第 1 记忆部（1412），用以存放可根据所述许可 Key 解密的所述

加密内容数据;

第 3 密钥保存部（1415），保存用以解密根据所述第 2 公开加密密钥所加密的数据的第 2 秘密解密密钥;

第 3 解密处理部（1416），用以依照所述第 2 解密处理部的解密结果，根据所述第 2 秘密解密密钥将所述许可 Key 解密.

2. 权利要求 1 记载的数据分发系统，其中，

所述分发数据解读部为可在所述终端拆装的存储插件;

所述第 1 秘密解密密钥为对应于所述存储插件的种类而预先确定的密钥;

所述第 2 秘密解密密钥按所述各存储插件而不同.

3. 权利要求 1 记载的数据分发系统，其中，

所述第 1 秘密解码密钥为对应于所述分发数据解读部的种类而预先确定的密钥;

所述第 2 秘密解密密钥按所述各分发数据解读部而不同.

4. 权利要求 2 记载的数据分发系统，其中，

所述第 2 及第 3 解密处理部，通过所述第 2 接口部接受在所述内容数据供给装置中以所述第 2 公开加密密钥所加密并以所述第 2 公用密钥再行加密且与所述许可 Key 一起分发的许可信息数据，并根据所述第 2 公用密钥及所述第 2 秘密解密密钥解密，

所述分发数据解读部还具备第 2 记忆部（1500），存放已解密的所述许可信息数据.

5. 权利要求 4 记载的数据分发系统，其中，

所述第 2 记忆部还存放由所述第 3 解密处理部所解密的所述许可 Key.

6. 权利要求 4 记载的数据分发系统，其中，

所述第 1 公用密钥和所述第 2 公用密钥为在所述加密内容数据的通信时由所述第 1 对话 Key 发生部所生成的同一密钥数据.

7. 权利要求 6 记载的数据分发系统，其中，

所述分发数据解读部还具备控制部，用以对应从外部所指示的再生动作模式判断能否根据所述第 2 记忆部所存放的许可信息数据进行再生并对所述分发数据解读部的动作加以控制，

所述第 1 加密处理部由所述控制部控制，对应指示所述内容数据

的再生动作，接受来自所述第 3 解密处理部的所述许可 Key，并根据第 3 公用密钥加密后输出，

所述第 1 记忆部由所述控制部控制，对应指示所述内容数据的再生动作，输出所述加密内容数据，

各所述终端还具备:

第 2 对话 Key 发生部（1502），生成在所述加密内容数据的每次通信时都被更新的所述第 3 公用密钥;

内容数据再生部（1506、1508），接受根据来自所述分发数据解读部的所述第 3 公用密钥所加密的所述许可 Key 进行解密和抽出，并根据所述许可 Key 将从所述第 1 记忆部所输出的所述加密内容数据解密并再生.

8. 权利要求 7 记载的数据分发系统，其中，

所述分发数据解读部还包含:

控制部（1420），用以对应向从外部所指示的其他终端转移所述加密内容数据及所述许可信息数据用的移动动作模式，对所述分发数据解读部的动作加以控制;

第 2 加密处理部（1414），用以用第 3 公开加密密钥进行加密处理，

所述第 2 解密处理部由所述控制部控制，对应指定所述移动动作模式，将根据所述第 3 公用密钥加密并从所述其他终端侧所发送的所述第 3 公开加密密钥解密并抽出，

所述第 2 加密处理部对应指定所述移动动作模式，以所述第 3 公开加密密钥将所述许可 Key 及所述许可信息数据加密，

所述第 1 加密处理部接受所述第 2 加密处理部的输出根据所述第 3 公用密钥进行加密，并提供给所述第 2 接口部，

所述控制部对应指定所述移动动作模式，将所述第 2 记忆部所存放的所述许可信息数据删除，

所述第 1 记忆部对应指定所述移动动作模式，将所述加密内容数据提供给所述第 2 接口部.

9. 权利要求 7 记载的数据分发系统，其中，

所述分发数据解读部还包含控制部，用以对应向从外部所指示的其他终端转移所述加密内容数据用的复制动作模式，对所述分发数据

解读部的动作加以控制，

所述第 1 记忆部对应指定所述复制动作模式，将所述加密内容数据提供给所述第 2 接口部。

10. 权利要求 4 记载的数据分发系统，其中，

所述分发数据解读部还包含：

第 3 对话 Key 发生部（1432），用以生成所述第 2 公用密钥；

第 3 加密处理部（1430），可以将所述第 3 对话 Key 发生部的输出加密并提供给所述第 2 接口部。

11. 权利要求 10 记载的数据分发系统，其中，

所述分发数据解读部还具备控制部，用以对应从外部所指示的再生动作模式判断能否根据所述第 2 记忆部所存放的许可信息数据进行再生并对所述分发数据解读部的动作加以控制，

所述第 3 加密处理部根据第 4 公开加密密钥将所述第 3 对话 Key 发生部的输出加密并提供给所述第 2 接口部；

所述第 1 加密处理部由所述控制部控制，对应指示所述内容数据的再生动作，接受来自所述第 3 解密处理部的所述许可 Key，并根据第 3 公用密钥加密后输出，

所述第 1 记忆部由所述控制部控制，对应指示所述内容数据的再生动作，输出所述加密内容数据，

各所述终端还具备：

第 2 对话 Key 发生部（1502），生成在所述加密内容数据的每次通信时都被更新的所述第 3 公用密钥；

公开密钥保存部（1524），将所述第 4 公开加密密钥提供给所述分发数据解读部；

公开密钥解密部（1522），能够将以所述第 4 公开加密密钥所加密的所述第 2 公用密钥解密；

内容数据再生部（1506、1508），接受根据来自所述分发数据解读部的所述第 3 公用密钥所加密的所述许可 Key 进行解密和抽出，并根据所述许可 Key 将从所述第 1 记忆部所输出的所述加密内容数据解密并再生。

12. 权利要求 11 记载的数据分发系统，其中，

所述分发数据解读部还包含：

控制部，用以对应向从外部所指示的其他终端转移所述加密内容数据及所述许可信息数据用的移动动作模式，对所述分发数据解读部的动作加以控制；

第 2 加密处理部，用以用第 3 公开加密密钥进行加密处理，

所述第 2 解密处理部由所述控制部控制，对应指定所述移动动作模式，将根据所述第 3 公用密钥加密并从所述其他终端侧所发送的所述第 3 公开加密密钥解密并抽出，

所述第 2 加密处理部对应指定所述移动动作模式，以所述第 3 公开加密密钥将所述许可 Key 及所述许可信息数据加密，

所述第 1 加密处理部接受所述第 2 加密处理部的输出根据所述第 3 公用密钥进行加密，并提供给所述第 2 接口部，

所述控制部对应指定所述移动动作模式，将所述第 2 记忆部所存放的所述许可信息数据删除，

所述第 1 记忆部对应指定所述移动动作模式，将所述加密内容数据提供给所述第 2 接口部。

13. 权利要求 11 记载的数据分发系统，其中，

所述分发数据解读部还包含控制部，用以对应向从外部所指示的其他终端转移所述加密内容数据用的复制动作模式，对所述分发数据解读部的动作加以控制，

所述第 1 记忆部对应指定所述复制动作模式，将所述加密内容数据提供给所述第 2 接口部。

14. 权利要求 1 记载的数据分发系统，其中，

所述第 1 接口部与所述第 2 接口部由便携式电话网所连接，

所述内容数据供给装置根据所述第 1 公开密码密钥对所述用户进行认证。

15. 权利要求 1 记载的数据分发系统，其中，

所述第 1 接口部包含可与所述终端直接连接的插接件部（2010）。

16. 权利要求 2 记载的数据分发系统，其中，

所述第 1 接口部包含可与所述存储插件直接连接的连接部（2030）。

17. 一种数据分发系统，用以从内容数据供给装置将加密内容数据和用以解密所述加密数据的许可 Key 中的至少其一分发给复数用户

的各终端，其中，

所述内容数据供给装置具备：

第 1 接口部（350），用以在与外部之间交换数据；

第 1 对话 Key 发生部（314），生成在所述加密内容数据的每次通信时都被更新的第 1 公用密钥；

对话 Key 加密处理部（316），用以根据对应于所述用户的终端所预先确定的第 1 公开加密密钥将所述第 1 公用密钥加密并提供给所述第 1 接口部；

对话 Key 解密部（318），将根据所述第 1 公用密钥加密并回送的第 2 公用密钥和第 2 公开加密密钥解密并抽出；

第 1 许可数据加密处理部（320），用以根据由所述对话 Key 解密部所解密的所述第 2 公开加密密钥将用以解密所述加密内容数据的许可 Key 加密；

第 2 许可加密处理部（322），用以将所述第 1 许可数据加密处理部的输出以所述第 2 公用密钥再行加密并提供给所述第 1 接口部进行分发，

各所述终端具备：

第 2 接口部，用以在与外部之间交换数据；

分发数据解读部（140），接受并存放所述加密内容数据及所述许可 Key；

所述分发数据解读部具备：

第 1 密钥保存部（1402），保存用以解密根据所述第 1 公开加密密钥所加密的数据的第 1 秘密解密密钥；

第 1 解密处理部（1404），用以接受根据所述第 1 公开加密密钥所加密的所述第 1 公用密钥并进行解密处理；

第 2 密钥保存部（1405），用以保存所述第 2 公开加密密钥；

第 2 对话 Key 发生部（1432），生成所述第 2 公用密钥；

第 1 加密处理部（1406），用以根据所述第 1 公用密钥将所述第 2 公开加密密钥和所述第 2 公用密钥加密并向所述第 2 接口部输出；

第 2 解密处理部（1410），用以接受来自所述第 2 许可数据加密处理部的已加密的许可 Key 并根据所述第 2 公用密钥进行解密；

记忆部，用以存放可用所述许可 Key 解密的加密内容数据；

第 3 密钥保存部（1415），保存用以解密根据所述第 2 公开加密密钥所加密的数据的第 2 秘密解密密钥；

第 3 解密处理部（1416），用以依照所述第 2 解密处理部的解密结果，根据所述第 2 秘密解密密钥将所述许可 Key 解密并抽出；

第 1 认证数据保存部（1442），对至少含有所述第 1 公开加密密钥的第 1 认证数据进行可根据公开认证密钥解密的加密并保存、并能够向外部输出，

所述内容数据供给装置还包含：

第 1 认证解密处理部（326），用以将能根据所述公开认证密钥解密且从外部提供的所述第 1 认证数据解密并抽出；

分发控制部（312），根据由所述第 1 认证解密处理部所抽出的所述第 1 认证数据进行认证处理，并判断是否至少分发许可 Key。

18. 权利要求 17 记载的数据分发系统，其中，

所述记忆部包含第 1 记忆单元（1412），用以存放由所述第 2 解密处理部所解密的结果、能够根据所述第 2 秘密解密密钥解密的状态的所述许可 Key 和所述加密内容数据。

19. 权利要求 17 记载的数据分发系统，其中，

所述记忆部包含：

第 1 记忆单元（1412），用以存放所述加密内容数据；

第 2 记忆单元（1500），用以存放由所述第 3 解密处理部所解密的所述许可 Key。

20. 权利要求 17 记载的数据分发系统，其中，

所述分发数据解读部为可在所述终端拆装的存储插件；

所述第 1 秘密解密密钥为对应于所述存储插件的种类而预先确定的值；

所述第 2 秘密解密密钥按所述各存储插件而不同。

21. 权利要求 17 记载的数据分发系统，其中，

所述第 1 秘密解密密钥为对应于所述分发数据解读部的种类而预先确定的值；

所述第 2 秘密解密密钥按所述各分发数据解读部而不同。

22. 权利要求 17 记载的数据分发系统，其中，

各所述终端还具备内容再生部，

所述内容再生部还包含第 2 认证数据保存部（1525），对至少含有预先确定的第 3 公开加密密钥的第 2 认证数据进行可根据所述公开认证密钥解密的加密并保存、并可向外部输出。

23. 权利要求 22 记载的数据分发系统，其中，

所述第 1 认证解密处理部，对已进行可以根据所述公开认证密钥解密的加密的所述第 2 认证数据再行解密并输出，

所述分发控制部根据在所述第 1 认证解密处理部所抽出的所述第 1 认证数据及所述第 2 认证数据进行认证处理，并判断是否至少分发许可 Key。

24. 权利要求 17 记载的数据分发系统，其中，

所述第 1 接口部与所述第 2 接口部由便携式电话网所连接。

25. 权利要求 17 记载的数据分发系统，其中，

所述第 1 接口部包含可与所述终端直接连接的插接件部。

26. 权利要求 20 记载的数据分发系统，其中，

所述第 1 接口部包含可与所述数据存放部直接连接的连接部。

27. 权利要求 26 记载的数据分发系统，其中，

所述分发数据解读部包含接受来自所述连接部的数据的复数端子（1462.0～1462.3），

按照来自外部的指令，从所述连接部接受数据的端子数能够切换。

28. 权利要求 22 记载的数据分发系统，其中，

所述记忆部接受所述第 2 解密处理部的输出，并存放已进行能够根据所述第 2 秘密解密密钥解密的加密的所述许可 Key，

所述内容再生部还具备：

第 4 密钥保存部（1520），用以保存将以所述第 3 公开加密密钥所加密的数据解密的第 3 秘密解密密钥；

第 4 解密处理部（1522），用以将在外部根据所述第 3 公开加密密钥所加密的第 2 公用密钥解密并抽出；

第 3 对话 Key 发生部（1502），生成第 3 公用密钥；

第 2 加密处理部（1504），用以根据在所述第 4 解密处理部解密并抽出的所述第 2 公用密钥将所述第 3 公用密钥加密并输出；

第 5 解密处理部（1506），用以将在所述内容再生部的外部根据

所述第 3 公用密钥所加密的许可 Key 解密并抽出；

数据再生部（1508），用以以所抽出的所述许可 Key 将所述记忆部所记录的加密内容数据解密并进行再生，

所述分发数据解读部还具备：

第 2 认证解密处理部（1452），用以将可根据所述公开认证密钥解密的、从所述内容再生部所提供的已加密的所述第 2 认证数据解密并抽出所述第 3 公开加密密钥；

第 3 加密处理部（1430），根据所述第 3 公开加密密钥将在所述第 2 对话 Key 发生部所生成的所述第 2 公用密钥加密；

控制部（1420），接受在所述内容再生部以所述第 2 公用密钥所加密的所述第 3 公用密钥，并根据在所述第 2 解密处理部（1410）基于所述第 2 公用密钥解密的所述第 3 公用密钥，将以所述第 2 秘密解密密钥对所述记忆部所存放的数据进行解密的所述许可 Key，在所述第 1 加密处理部进行加密，并指示向所述内容再生部输出，

所述控制部根据由所述第 2 认证解密处理部所解密的所述第 2 认证数据进行认证处理，并判断是否至少输出许可 Key。

29. 权利要求 20 记载的数据分发系统，其中，

所述记忆部接受所述第 2 解密处理部的输出，存放已进行能够根据所述第 2 秘密解密密钥解密的加密的所述许可 Key，

所述分发数据解读部还包含：

第 2 认证解密处理部（1452），为了向其他终端的分发数据解读部至少转移所述许可 Key，对应从所述分发数据解读部的外部所指示的移动处理，将能够根据来自所述其他分发数据解读部的所述公开认证密钥解密的已加密的第 1 认证数据以所述公开认证密钥解密并抽出所述其他分发数据解读部的所述第 1 公开加密密钥；

第 3 加密处理部（1430），用以根据所述其他分发数据解读部的所述第 1 公开加密密钥将所述第 2 公用密钥加密；

第 4 加密处理部（1414），用以进行依据所述其他分发数据解读部的第 2 公开加密密钥的加密处理，

所述第 2 对话 Key 发生部对应所述移动处理，产生所述第 2 公用密钥，

所述第 2 解密处理部对应所述移动处理，将从所述其他分发数据

解读部根据所述第 2 公用密钥所加密并输入的第 4 公用密钥和所述其他分发数据解读部的第 2 公开加密密钥解密并抽出，

所述第 3 解密处理部对应所述移动处理，根据所述第 2 秘密解密密钥将以所述记忆部所存放的所述第 2 公开加密密钥所加密的数据解密并抽出许可 Key，

所述第 4 加密处理部对应所述移动处理，根据所述其他分发数据解读部的第 2 公开加密密钥将所抽出的所述许可 Key 加密，

所述第 1 加密处理部对应所述移动处理，将所述第 4 加密处理部的输出以所述第 4 公用密钥加密并向所述其他分发数据解读部输出，

所述控制单元根据由所述第 2 认证解密处理部所抽出的并从所述其他数据解读部所输出的第 2 认证数据进行认证处理，并判断是否至少输出许可 Key。

30. 权利要求 29 记载的数据分发系统，其中，

所述其他分发数据解读部，在所述认证解密处理中对应用以从所述分发数据解读部至少转移所述许可 Key 的从所述其他分发数据解读部的外部所指示的移动处理，所述第 1 认证数据保存部输出所述第 1 认证数据，

所述第 1 解密处理部对应所述移动处理，将从所述分发数据解读部根据所述第 1 公开加密密钥加密并输入的、在所述分发数据解读部所产生的所述第 2 公用密钥解密并抽出，

所述第 2 对话 Key 发生部对应所述移动受理处理，产生所述第 4 公用密钥，

所述第 1 加密处理部对应所述移动受理处理，根据第 2 公用密钥将所述第 2 公开加密密钥和所述第 4 公用密钥加密并输出，

所述第 2 解密处理部将在所述分发数据解读部中以所述第 2 公开加密密钥所加密并以所述第 4 公用密钥再行加密的许可 Key 以所述第 4 公用密钥解密并记录于所述记忆部。

31. 权利要求 26 记载的数据分发系统，其中，

所述内容数据供给装置还包含：

第 5 密钥保存部，保存与所述内容再生部通用的第 5 公用密钥；

第 3 许可加密部，根据所述第 5 密钥保存部所保存的所述第 5 公用密钥，将所述许可 Key 加密并向所述第 1 许可加密处理部输出，

所述内容再生部还包含:

第 6 密钥保存单元，保存所述第 5 公用密钥;

第 5 解密处理部，设置于所述第 4 解密处理部与所述数据再生部之间，并根据所述第 6 密钥保存部所保存的所述第 5 公用密钥，从所述第 4 解密处理部的输出将所述许可 Key 解密并抽出，并向所述数据再生部输出.

32. 权利要求 26 记载的数据分发系统，其中，

所述内容数据供给装置还包含:

第 5 密钥保存部，保存能够在所述内容再生部解密的第 4 公开加密密钥;

第 3 许可加密部，根据第 4 公开加密密钥将所述许可 Key 加密并在所述第 1 许可加密处理部输出，

所述内容再生部还包含:

第 6 密钥保存单元，保存可以将根据第 4 公开加密密钥所加密的数据解密的第 4 秘密解密密钥;

第 5 解密处理部，设置于所述第 4 解密处理部与所述数据再生部之间并根据第 4 秘密解密密钥从所述第 4 解密处理部的输出将所述许可 Key 解密并抽出，并向所述数据再生部输出.

33. 权利要求 20 记载的数据分发系统，其中，

所述终端具备复数个分发数据解读部.

数据分发系统

技术领域

本发明涉及用于向便携式电话机等终端分发信息的数据分发系统，更确定地说是涉及能够对所拷贝的信息进行版权保护的数据分发系统。

现有技术

近几年，由于因特网等信息通信网的进步，各用户凭借使用便携式电话机等的面向人个的终端对网络信息进行轻松访问也成为可能。

在这样的信息通信中信息是通过数字信号来传送的。因此，比如在每个个人用户对在象上述的信息通信网中所传送的音乐和影像信息进行了拷贝时，也几乎不会产生这样的拷贝带来的音质和画质的劣化就可以进行信息的拷贝。

因此，在这样的信息通信网中传送具有音乐信息和图像信息等版权的创作作品时，如果不采取妥当的版权保护措施，恐怕会导致版权者的权利受到显著的侵害。

另一方面，如果把保护版权的目的放在第一位，而不能通过迅速扩大的数字信息通信网进行作品数据的分发，这基本上对于在复制作品时可以收取一定版权费用的版权者来说反而是不利的。

在这里，且不考虑通过上述数字信息通信网进行的分发，而以记录有数字信息的记录媒体为例来考虑的话，关于通常销售的记录有音乐信息的 CD（袖珍激光唱盘），从 CD 向磁光盘（MD 等）拷贝音乐数据，只要该拷贝的音乐限于为个人使用，在原则上是可以自由进行的。不过，进行数字录音等的个人用户要将数字录音设备本身和 MD 等媒体的价款中的一定数额作为补偿金间接地支付给版权者。

然而，在从 CD 向 MD 拷贝了数字信息的音乐信息时，鉴于这些信息是几乎不会因拷贝而劣化的数字信息，为了保护版权者，在机器的结构上是不能将音乐数据作为数字信息从一个 MD 再向其他 MD 进行拷贝的。

也就是说，在现状下从数字记录媒体的 CD 向 MD 的拷贝在从母盘

到子盘时可以自由进行，但是从能够记录的 MD 向 MD 的拷贝却不能进行。

从如此情况来看，通过数字信息通信网向公众分发音乐数据和图像数据，这本身就是受版权者的公众发送权限制的行为，所以有必要采取充分的措施以保护版权。

这种情况下，防止本来没有接收权限的用户接收通过信息通信网向公众发送的作品数据当然是必要的，即使是有权限的用户进行了接收时，也有必要防止一度被接收的作品再被随便复制。

发明内容

本发明的目的是提供一个在通过信息通信网例如便携式电话机等的信息通信网分发作品数据时，仅具有正当访问权的用户才能接收这样信息的信息分发系统。

此发明的其他目的是提供一个能防止所分发的作品数据未经版权者许可而被复制的信息分发系统。

为实现这样的目的，本申请之发明相关的数据分发系统是用以从内容数据供给装置向复数用户的各终端分发加密内容数据的数据分发系统。

内容数据供给装置具备第 1 接口部、第 1 对话 Key 发生部、对话 Key 加密部、对话 Key 解密部、第 1 许可数据加密处理部、第 2 许可数据加密处理部。

第 1 接口部在与外部之间进行数据交换。

第 1 对话 Key 发生部生成每次加密内容数据通信时都被更新的第 1 公用密钥。对话 Key 加密部根据对应于用户终端而预先设定的第 1 公开加密密钥对第 1 公用密钥进行加密后传给第 1 接口部。对话 Key 解密部对根据第 1 公用密钥加密并回送的数据进行解密。

第 1 许可数据加密处理部将对话 Key 解密部所解密的数据作为密钥数据对用于解密加密内容数据的许可 Key 进行加密。第 2 许可数据加密处理部用第 2 公用密钥对第 1 许可数据加密处理部的输出再加密后提供给第 1 接口部并分发。

各终端具备第 2 接口部和分发数据解读部。

第 2 接口部在与外部之间进行数据交换。

分发数据解读部接受并存放加密内容数据。分发数据解读部具备第 1 密钥保存部、第 1 解密处理部、第 2 密钥保存部、第 1 加密处理部、第 2 解密处理部、第 1 记忆部、第 3 密钥保存部、第 3 解密处理部。

第 1 密钥保存部，保存用以解密根据第 1 公开加密密钥所加密的数据的第 1 秘密解密密钥。第 1 解密处理部接受根据第 1 公开加密密钥加密的第 1 公用密钥进行解密处理。

第 2 密钥保存部保存第 2 公开加密密钥。第 1 加密处理部根据第 1 公用密钥对第 2 公开加密密钥进行加密并输出至第 2 接口部。

第 2 解密处理部接受来自第 2 许可数据加密处理部的已加密的许可 Key，并根据第 2 公用密钥进行解密。

第 1 记忆部存放可以根据许可 Key 进行解密的所述加密内容数据。

第 3 密钥保存部保存用于对根据第 2 公开加密密钥加密的数据进行解密的第 2 秘密解密密钥。第 3 解密处理部用于根据第 2 解密处理部的解密结果，由第 2 秘密解密密钥对许可 Key 进行解密。

再依照此发明的其他方面，则为一个用以将加密内容数据和用于对加密数据进行解密的许可 Key 中的至少其一从内容数据供给装置向复数用户的各终端分发的数据分发系统。

内容数据供给装置具备第 1 接口部、第 1 对话 Key 发生部、对话 Key 加密处理部、对话 Key 解密部、第 1 许可数据加密处理部、第 2 许可加密处理部。

第 1 接口部在与外部之间进行数据交换。

第 1 对话 Key 发生部生成每次加密内容数据通信时都被更新的第 1 公用密钥。对话 Key 加密处理部根据对应于用户终端而预先设定的第 1 公开加密密钥对第 1 公用密钥加密后传给第 1 接口部。对话 Key 解密部对根据第 1 公用密钥加密并回送的第 2 公用密钥和第 2 公开加密密钥进行解密并抽出。

第 1 许可数据加密处理部根据对话 Key 解密部所解密的第 2 公开加密密钥对用于解密加密内容数据的许可 Key 进行加密。第 2 许可加密处理部用第 2 公用密钥对第 1 许可数据加密处理部的输出再行加密后提供给第 1 接口部并分发。

各终端具备第 2 接口部和分发数据解读部.

第 2 接口部在与外部之间进行数据交换.

分发数据解读部接受并存放加密内容数据及许可 Key.

分发数据解读部具备第 1 密钥保存部、第 1 解密处理部、第 2 密钥保存部、第 2 对话 Key 发生部、第 1 加密处理部、第 2 解密处理部、记忆部、第 3 密钥保存部、第 3 解密处理部、第 1 认证数据保存部.

第 1 密钥保存部保存用于对根据第 1 公开加密密钥加密的数据进行解密的第 1 秘密解密密钥. 第 1 解密处理部接受根据第 1 公开加密密钥加密的第 1 公用密钥并进行解密处理.

第 2 密钥保存部保存第 2 公开加密密钥. 第 2 对话 Key 发生部生成第 2 公用密钥.

第 1 加密处理部根据第 1 公用密钥对第 2 公开加密密钥和第 2 公用密钥进行加密并输出至第 2 接口部. 第 2 解密处理部接受来自第 2 许可数据加密处理部的加密了的许可 Key 并根据第 2 公用密钥进行解密. 记忆部存放可以用许可 Key 进行解密的加密内容数据.

第 3 密钥保存部保存用以对根据第 2 公开加密密钥加密的数据进行解密的第 2 秘密解密密钥. 第 3 解密处理部根据第 2 解密处理部的解密结果, 由第 2 秘密解密密钥对许可 Key 进行解密并抽出. 第 1 认证数据保存部对至少含有第 1 公开加密密钥的第 1 认证数据进行可根据公开认证密钥解密的加密并保存, 并可向外部输出.

内容数据供给装置还包括第 1 认证解密处理部, 可凭借公开认证密钥进行解密并用以对外部提供的第 1 认证数据进行解密并抽出; 分发控制部, 根据第 1 认证解密处理部所抽出的第 1 认证数据进行认证处理且判断是否至少进行许可 Key 的分发.

因此, 凭借本发明, 仅使正规的用户可接收内容数据并存放于存储器中. 而且, 要将一度存放于存储插件中的数据让他人拷贝时, 该他人若想在可再生状态下转移数据, 在结构上将在发送源致使数据不能再生, 所以可以防止由无限制的拷贝而使版权者蒙受的不正当的损害.

此发明的其他优点是, 由于许可 Key 只分发给被认证的终端, 所以将进一步强化版权的保护.

此发明再其他的优点是, 用户不用通过分发媒体而可以通过内容

数据销售机来购入加密内容数据，所以将进一步提高用户的便利性。

附图说明

图 1 为用以对本发明的信息分发系统的整体结构进行概略说明的概念图。

图 2 为在图 1 所示的信息分发系统中使用的通信用 Key 数据（密钥数据）等的特性的总结说明图。

图 3 为表示图 1 所示之分发服务器 10 的结构的概略框图。

图 4 为用以说明图 1 所示之便携式电话机 100 的结构的概略框图。

图 5 为用以说明图 4 所示之存储插件 110 的结构的概略框图。

图 6 为用以说明在图 1 及图 3～图 5 说明的数据分发系统中的分发模式的第 1 流程图。

图 7 为用以说明在图 1 及图 3～图 5 说明的数据分发系统中的分发模式的第 2 流程图。

图 8 为对用以在便携式电话机 100 内再生内容数据并作为音乐输出至外部的再生处理加以说明的流程图。

图 9 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 1 流程图。

图 10 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 2 流程图。

图 11 为表示与实施方式 2 的存储插件 120 对应的音乐服务器 31 结构的概略框图。

图 12 为用以说明实施方式 2 中的便携式电话机 101 结构的概略框图。

图 13 为用以说明本发明实施方式 2 的存储插件 120 结构的概略框图。

图 14 为用以说明采用了在图 13 说明的存储插件 120 的分发模式的第 1 流程图。

图 15 为用以说明采用了在图 13 说明的存储插件 120 的分发模式的第 2 流程图。

图 16 为对用以在便携式电话机 101 内再生内容数据并作为音乐输出至外部的再生处理加以说明的第 1 流程图。

图 17 为对用以在便携式电话机 101 内再生内容数据并作为音乐输出至外部的再生处理加以说明的第 2 流程图.

图 18 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 1 流程图.

图 19 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 2 流程图.

图 20 用以说明实施方式 3 的数据分发系统的结构的概念图.

图 21 为表示实施方式 3 的内容数据销售机 2000 的结构的概略框图.

图 22 为用以说明在图 20 及图 21 说明的数据分发系统中的分发模式的第 1 流程图.

图 23 为用以说明在图 20 及图 21 说明的数据分发系统中的分发模式的第 2 流程图.

图 24 为表示实施方式 3 的变化例的内容数据销售机 2001 的结构的概念图.

图 25 为用以说明实施方式 3 的变化例的数据分发系统中的分发模式的第 1 流程图.

图 26 为用以说明实施方式 3 的变化例的数据分发系统中的分发模式的第 2 流程图.

图 27 为用以说明实施方式 4 的内容数据销售机 3000 的结构的概略框图.

图 28 为用以说明在图 27 说明的数据分发系统中的分发模式的第 1 流程图.

图 29 为用以说明在图 27 说明的数据分发系统中的分发模式的第 2 流程图.

图 30 为用以说明实施方式 4 的变化例的数据分发系统中的分发模式的第 1 流程图.

图 31 为用以说明实施方式 4 的变化例的数据分发系统中的分发模式的第 2 流程图.

图 32 为用以说明实施方式 5 中的便携式电话机 105 的结构的概略框图.

图 33 为表示与实施方式 5 的存储插件 140 对应的分发服务器 12

的结构的概略框图.

图 34 为用以说明本发明的实施方式 5 的存储插件 140 的结构的概略框图.

图 35 为用以说明采用了存储插件 140 的分发模式的第 1 流程图.

图 36 为用以说明采用了存储插件 140 的分发模式的第 2 流程图.

图 37 为对用以从存储插件 140 所保存的加密内容数据作为音乐输出至外部的再生处理进行说明的第 1 流程图.

图 38 为对用以从存储插件 140 所保存的加密内容数据作为音乐输出至外部的再生处理进行说明的第 2 流程图.

图 39 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 1 流程图.

图 40 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 2 流程图.

图 41 为表示本发明实施方式 6 的内容数据销售机 3010 的结构的概略框图.

图 42 为用以说明采用了内容数据销售机 3010 的数据分发系统中的分发模式的第 1 流程图.

图 43 为用以说明采用了内容数据销售机 3010 的数据分发系统中的分发模式的第 2 流程图.

图 44 为用以说明实施方式 7 中的便携式电话机 107 的结构的概略框图.

图 45 为表示与实施方式 7 的便携式电话机 107 对应的分发服务器 13 的结构的概略框图.

图 46 为用以说明采用了分发服务器 12 和便携式电话机 107 的分发模式的第 1 流程图.

图 47 为用以说明采用了分发服务器 12 和便携式电话机 107 的分发模式的第 2 流程图.

图 48 为对用于从存储插件 140 所保存的加密内容数据作为音乐输出至外部的再生处理进行说明的第 1 流程图.

图 49 为对用以从存储插件 140 所保存的加密内容数据作为音乐输出至外部的再生处理进行说明的第 2 流程图.

图 50 为用以说明在实施方式 7 的两个存储插件之间进行内容数据

及 Key 数据等的移动或复制处理的第 1 流程图.

图 51 为用以说明在实施方式 7 的两个存储插件之间进行内容数据及 Key 数据等的移动和复制处理的第 2 流程图.

图 52 为表示本发明实施方式 8 的内容数据销售机 3020 的结构的概略框图.

图 53 为用以说明采用了内容数据销售机 3020 的数据分发系统中的分发模式的第 1 流程图.

图 54 为用以说明采用了内容数据销售机 3020 的数据分发系统中的分发模式的第 2 流程图.

图 55 为说明存储插件 140 的端子 1202 部分的结构的概略框图.

图 56 为说明存储插件 140 的端子 1202 部分的结构的变化例的概略框图.

实施方式

下面，结合附图对本发明的实施例作以说明.

[实施例 1]

[系统的整体结构]

图 1 为用以对本发明的信息分发系统的整体结构进行概略说明的概念图.

另外，以下以通过便携式电话网将音乐数据分发给各用户的数据分发系统的结构为例进行说明，但正如以下的说明中所明确的那样，本发明并不局限于此种情况，也可应用于通过其他信息通信网对其他作品数据例如图像数据等作品数据进行分发的情况.

参照图 1，对存在版权的音乐信息进行管理的分发服务器 10 按照规定的密码方式对音乐数据（以下也称内容数据）进行加密后，将此加密数据提供给分发信息用的分发媒体 20——便携式电话机公司. 另一方面，认证服务器 12 对于请求音乐数据分发而来访的机器是否为正规的机器进行认证.

分发媒体 20 通过自身的便携式电话网将来自各用户的分发要求（分发请求）中转给分发服务器 10. 当有配线请求时，分发服务器 10 依据认证服务器 12 确认其为来自正规机器的访问，并对所要求的内容数据再行加密后通过分发媒体 20 的便携式电话网对各用户的便携式电

话机进行分发.

图 1 中，例如便携式电话机用户 1 的便携式电话机形成这样的结构：接受便携式电话机 100 所收到的加密内容数据后对在上述发送之际进行的加密施以解密，并将其存放于可拆装的存储插件 110 中以提供给便携式电话机 100 中的音乐再生部（图中未示）.

进而，例如用户 1 可以通过连接于便携式电话机 100 的耳机 130 等听到对该内容数据再生得到的音乐.

以下将该分发服务器 10、认证服务器 12 和分发媒体 20 合并，统称为音乐服务器 30.

另外，将从该音乐服务器 30 向各便携式电话机终端等传送内容数据的处理称作“分发”.

通过形成这样的结构，首先，未购买正规的存储插件——存储插件 110 的非正规用户，在结构上难以从音乐服务器 30 接受分发数据并再生.

而且，在分发媒体 20 中，例如在每分发一曲的内容数据时都计算该次数，据此分发媒体 20 若将每次用户接收内容（下载）时发生的版权费作为便携式电话机的通话费用进行收取的话，版权者确保版权费用就容易了.

而且，这样的内容数据的分发是通过便携式电话网这一封闭的系统进行的，所以与因特网等开放式系统相比，有容易采取版权保护对策的优点.

这时，例如拥有存储插件 112 的用户 2 可以通过自己的便携式电话机 102 从音乐服务器 30 直接接受内容数据的分发. 然而，如果用户 2 欲直接从音乐服务器 30 接收相当大信息量的内容数据等，有时要花很长时间用于接收. 这种情况下，如果可以从已经接受该内容数据分发的用户 1 处拷贝该内容数据，将提高用户的便利性.

但是，从保护版权者权利的观点出发，在系统的结构上不允许内容数据的拷贝放任自由.

在图 1 的示例中，在与内容数据本身及为使该内容数据能够再生所必要的信息一起，将用户 1 所接收的内容数据拷贝给用户 2 时称为内容数据的“移动”. 这时，用户 1 要将用于再生的必要信息（再生信息）逐个拷贝给用户 2，就有必要在进行信息移动后使用户 1 不能进

行内容数据的再生。在这里，内容数据作为按照规定的加密方式加密的加密内容数据被分发，所谓的“再生信息”如下文说明，为可以按照上述规定的加密方式对加密内容数据进行解密的密钥（也称许可Key）和关系到版权保护的信息的许可ID数据及用户ID数据等许可信息。

与此相对，仅将内容数据在加密状态下拷贝给用户2，称之为音乐信息的“复制”。

这时，用户2的终端未拷贝到再生该内容数据所必要的再生信息，所以用户2仅得到加密内容数据是不能再生音乐的。因此，用户2在希望再生该音乐时，需要重新从音乐服务器30处接受可进行内容数据再生用的再生信息的分发，所以与用户2直接从音乐服务器30接受全部分发相比，可以用格外短的通话时间使音乐再生成为可能。

例如，便携式电话机100和102为PHS（Personal Handy Phone）时，可以进行所谓的无线电收发报机模式的通话，所以利用该功能可以进行用户1到用户2的总括信息的转移（移动）和仅为加密内容数据的传送（复制）。

在图1所示结构中，为使经过加密并分发的内容数据可在用户一侧再生，在系统上所必要的是：第1，为用以分发通信中的加密Key（密钥）的方式；第2，为对分发数据加密的方式本身；第3，为实现用以防止对如此分发的数据进行擅自拷贝的数据保护的结构。

[密码/解密密钥的结构]

图2为在图1所示信息分发系统中所使用的通信用Key数据（密钥数据）等的特性的总结说明图。

首先，在图1所示结构中，作为存储插件100内的用于管理数据处理的密钥，是存储插件这种媒体的种类中固有的，且有包含个别指定存储插件种类等所用信息的秘密解密密钥Kmedia(n)（n：自然数）、依各存储插件而不同的公开加密密钥KPcard(n)、对根据公开加密密钥KPcard(n)加密的数据进行解密所用的秘密解密密钥Kcard(n)。

在此，密钥Kcard(n)和密钥KPcard(n)的表记中的自然数n表示用以区别各存储插件的号码。

也就是说，以公开加密密钥KPcard(n)加密的数据可以用各存储插件中存在的秘密解密密钥Kcard(n)进行解密。因此，在存储插件的

分发数据的交换中基本上要使用如后述说明的三个密码密钥 Kmedia(n) 、Kcard(n)、KPcard(n)。

另外，作为在存储插件外部和存储插件之间的数据交换中的秘密保存用的密码密钥，将用到各媒体固有的公开加密密钥 KPmeida(n)、用以对根据公开加密密钥KPmedia(n)加密的数据进行解密的秘密解密密钥 Kmeida(n)、在每次通信例如用户每次访问音乐服务器 30 时在音乐服务器 30、便携式电话机 100 或 102 中生成的公用密钥 Ks。

在此，公用密钥 Ks 形成例如在用户每访问一次音乐服务器 30 就产生的结构，也可形成只是一次访问对多少曲音乐信息都使用同一公用密钥的结构，或者可以形成例如按各曲目变更该公用密钥并在每次分发给用户的结构。

以下将这种通信单位或访问单位称为“对话”，将公用密钥 Ks 称为“对话 Key”。

因此，公用密钥 Ks 在各通信对话具有固有值，并在分发服务器和便携式电话机中得到管理。

另外，关于将要分发的数据，首先有加密内容数据进行解密的密钥 Kc（以下称许可 Key），依据该许可 Key Kc 对加密内容数据进行解密。另外，作为上述许可信息，有可指定该当内容数据的管理代码和含有限制再生次数等信息的许可 ID 数据 License-ID 等。另一方面，便携式电话机保存有用以识别接收者的用户 ID 数据 User-ID。

通过形成这样的结构，对应许可 ID 数据中所含有的信息，能够进行有关版权者侧的版权保护的控制，另一方面通过使用用户 ID 数据，能够控制用户个人信息的保护，例如使局外人难以知道用户的访问历史记录等。

分发数据中的内容数据 Dc，如上所述例如是音乐数据，将可以用许可 Key Kc 对该内容数据进行解密的数据称为加密内容数据[Dc]Kc。

在此，表记[Y]X 表示将数据 Y 转换成可依据 Key（密钥）X 进行解密的密码的数据。另外，在加密处理、解密处理中使用的密钥也称作“Key”。

[分发服务器 10 的结构]

图 3 为表示图 1 所示分发服务器 10 的结构的概略框图。分发服务器 10 具备：分发信息数据库 304，用以保存将内容数据（音乐数据）

按照规定的方式加密的数据和许可 ID 等分发信息；收费数据库 302，用以保存依从于各个用户分别对内容数据的访问次数等的收费信息；数据处理部 310，用以通过数据总线 BS1 接受来自分发信息数据库 304 及收费信息数据库 302 的数据并进行规定的加密处理；通信装置 350，用以通过通信网在分发媒体 20 和数据处理部 310 之间进行数据交换。

数据处理部 310 包括：分发控制部 312，对应数据总线 BS1 上的数据，用以控制数据处理部 310 的动作；对话 Key 发生部 314，由分发控制部 312 控制，用以产生对话 Key Ks；加密处理部 316，用以根据公开加密密钥 KPmeida 对对话 Key 发生部 314 所生成的对话 Key Ks 进行加密并提供给数据总线 BS1；解密处理部 318，通过通信装置 350 及数据总线 BS1 接受各用户的便携式电话机中按照对话 Key Ks 加密后所发送的数据，并进行解密处理；加密处理部 320，使用解密处理部 318 所抽出的公开加密密钥 KPcard(n)，由分发控制部 312 控制用以对许可 Key 和许可 ID 等数据进行加密；加密处理部 322，再根据对话 Key Ks 对加密处理部 320 的输出进行加密、通过数据总线 BS1 提供给通信装置 350。

[终端（便携式电话机）的结构]

图 4 为用以说明图 1 所示便携式电话机 100 的结构的概略框图。

便携式电话机 100 具备：天线 1102，用以接收由便携式电话网所无线传送的信号；收发信部 1104，用以接受来自天线 1102 的信号并转换为基带信号、或对来自便携式电话机的数据进行调制并提供给天线 1102；数据总线 BS2，用以进行便携式电话机 100 的各部数据交换；控制器 1106，用以通过数据总线 BS2 控制便携式电话机 100 的动作；用户 ID 保存部 1107，保存用以识别接收者的用户 ID 数据 User-ID；接触密钥部 1108，用以将来自外部的指示提供给便携式电话机 100；显示器 1110，用以将控制器 1106 等所输出的信息作为视觉信息提供给用户；语音再生部 1112，用以在通常的通话操作中，根据通过数据总线 BS2 提供的接收数据再生语音；插接件 1120，用以与外部之间进行数据交换；外部接口部 1122，用以将来自插接件 1120 的数据转换为可以提供给数据总线 BS2 的信号或将来自数据总线 BS2 的数据转换为可以提供给插接件 1120 的信号。

在此，用户 ID 数据含有例如用户的电话号码等数据。

便携式电话机100还包括：可拆装存储插件110，用以对来自音乐服务器30的内容数据进行解密处理；存储器接口1200，用以控制存储插件110和数据总线BS2之间的数据交换；对话Key发生部1502，在存储插件110与便携式电话机的其他部分的数据交换时，依据随机数等产生用以对数据总线BS2上所交换的数据进行加密的对话Key Ks；加密处理部1504，用以对对话Key发生部1502所生成的对话Key进行加密并提供给数据总线BS2；解密处理部1506，根据对话Key Ks对对话Key发生部1502所生成的、数据总线BS2上的数据进行解密并输出；音乐再生部1508，用以接受解密处理部1506的输出并再生音乐信号；混合部1510，用以接受音乐再生部1508的输出和语音再生部1112的输出并对应动作模式有选择地输出；数模转换部1512，接受混合部1510的输出并将其转换为用于向外部输出的模拟信号；连接端子1514，用以接受数模转换部1512的输出并与耳机130连接。

另外，为使说明简洁仅对本发明的内容数据的分发的相关区段作以记载，关于便携式电话机本来具备的通话功能的相关区段则有所割爱。

[存储插件的结构]

图5为用以说明图4所示存储插件110的结构的概略框图。

以下对装设于终端100的存储插件110的公开加密密钥Kpmedia与装设于终端102的存储插件112的公开加密密钥KPmedia加以区别，分别将存储插件110所对应者称作公开加密密钥KPmedia（1）、将存储插件112所对应者称作公开加密密钥KPmedia（2）。

另外，与此对应，将能对用公开加密密钥KPmedia（1）加密的数据进行解密并与之非对称的秘密解密密钥称作秘密解密密钥Kmedia（1），将能对用公开加密密钥KPmedia（2）加密的数据进行解密并与之非对称的秘密解密密钥称作秘密解密密钥Kmedia（2）。

这样，根据对媒体固有的公开加密密钥的区别，如以下说明中明确的，在存储插件存在复数种类时，以及更一般性地，在存储插件以外的媒体作为系统的可选项而存在时，也可进行对应。

存储插件110具备：数据总线BS3，通过端子1202与存储器接口1200进行信号交换；KPmedia（1）保存部1401，用以保存公开加密密钥KPmedia（1）的值并将公开加密密钥KPmedia（1）输出至数据总线

BS3; Kmedia（1）保存部1402，用以保存对应于存储插件110的秘密解密密钥Kmedia(1);解密处理部1404,通过根据秘密解密密钥Kmedia（1）进行的解密处理，从存储器接口1200提供给数据总线BS3的数据中抽出对话Key Ks; KPcard(1)保存部1405，用以保存公开加密密钥KPcard(1)；加密处理部1406，用以根据解密处理部1404所抽出的对话Key Ks对切换开关1408的输出进行加密并提供给数据总线BS3;解密处理部1410，用以根据解密处理部1404所抽出的对话Key Ks对数据总线BS3上的数据进行解密处理并提供给数据总线BS4；存储器1412，用以从数据总线BS4存放以各存储插件不同的公开加密密钥KPcard(n)进行加密的许可Key Kc、许可ID等数据并从数据总线BS3接受并存放按照许可Key Kc加密的加密内容数据[Dc]Kc.

切换开关1408具有接点Pa、Pb、Pc,其数据提供为:来自KPcard(1)保存部1405的公开加密密钥KPcard(1)提供给接点Pa；数据总线BS5提供给接点Pb;加密处理部1414的输出提供给接点Pc.切换开关1408按照其动作模式为“分发模式”、“再生模式”、“移动模式”中的哪一种，分别将提供给接点Pa、Pb、Pc的信号有选择地提供给加密处理部1406.

存储插件110还具备: Kcard(1)保存部1415，用以保存秘密解密密钥Kcard(1)的值;解密处理部1416,对根据公开加密密钥KPcard(1)进行加密且从存储器1412读出的许可Key Kc、许可ID等的（[Kc、License]Kcard(1)）进行解密处理并提供给数据总线BS5；加密处理部1414，在数据的移动处理等中，用以从解密处理部1410接受目标地存储插件的公开加密密钥KPcard(n)并根据该目标的公开加密密钥KPcard(n)对输出至数据总线BS5上的许可Key Kc、许可ID等进行加密后，输出至切换开关1408；控制器1420，用以通过数据总线BS3与外部进行数据交换并在与数据总线BS5之间接受许可ID数据等，控制存储插件110的动作；寄存器1500，在与数据总线BS5之间能进行许可ID数据等数据交换.

另外，图5中由实线所围的范围被组入用以在存储插件110中受到外部的不正当开封处理等时通过删除内部数据和破坏内部电路而使第三者不能读出存在于该范围内的数据等的模块TRM中.

这样的模块一般称为防窜改模块（Tamper Resistance Module）.

当然，也可以为包括存储器 1412 组入模块 TRM 内的结构。但是，通过图 5 所示的结构，因为存储器 1412 中所保存的数据皆为加密数据，所以第三者只凭该存储器 1412 中的数据不可能再生音乐，且没有必要将存储器 1412 设置在昂贵的防窜改模块之内，从而有降低制造成本的优点。

图 6 及图 7 为用以对图 1 及图 3～图 5 所说明的数据分发系统中的分发动作进行说明的第 1 及第 2 流程图。

在图 6 及图 7 中，对用户 1 通过使用存储插件 110 从音乐服务器 30 接受音乐数据的分发时的动作进行说明。

首先，从用户 1 的便携式电话机 100 由用户通过进行接触 Key1108 的按密钥操作等发出分发请求（步骤 S100）。

在存储插件 110 中，对应该分发请求将公开加密密钥 KPmedia(1) 从 KPmedia(1) 保存部 1401 发送给音乐服务器 30（步骤 S102）。

在音乐服务器 30 中，接收从存储插件 110 所传递的分发请求及公开加密密钥 KPmedia(1) 时（步骤 S104），根据接收到的公开加密密钥 KPmedia(1) 向认证服务器 12 进行查询，当为来自正规存储插件的访问时移交下一步处理（步骤 S106），当为非正规存储插件时结束处理（步骤 S154）。

查询的结果，当确认为正规存储插件时，在音乐服务器 30 中，对话 Key 发生部 314 生成对话 Key Ks。进而，音乐服务器 30 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1) 将该对话 Key Ks 加密并生成加密对话 Key[Ks]Kmedia(1)（步骤 S108）。

接下来，音乐服务器 30 将加密对话 Key[Ks]Kmedia(1) 提供给数据总线 BS1。通信装置 350 通过通信网向便携式电话机 100 的存储插件 110 发送来自加密处理部 316 的加密对话 Key[Ks]Kmedia(1)（步骤 S110）。

便携式电话机 100 接收加密对话 Key[Ks]Kmedia(1) 后（步骤 S112），在存储插件 110 中，解密处理部 1404 根据秘密解密密钥 Kmedia(1) 对通过存储器接口 1200 提供给数据总线 BS3 的接收数据进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S114）。

接下来，在分发动作中，切换开关 1408 的接点 Pa 选择闭合状态，所以加密处理部 1406 根据对话 Key Ks 对通过接点 Pa 由 KPcard(1)

保存部 1405 提供的公开加密密钥 KPcard(1)（对于存储插件 110 的公开加密密钥）进行加密（步骤 S116），生成数据[KPcard(1)]Ks（步骤 S118）.

便携式电话机 100 将加密处理部 1406 所加密的数据[KPcard(1)]Ks 发送给音乐服务器 30（步骤 S120）.

在音乐服务器 30 中，由通信装置 350 接收数据[KPcard(1)]Ks(步骤 S122），解密处理部 318 根据对话 Key Ks 对提供给数据总线 BS1 的数据[KPcard(1)]Ks 进行解密处理，将公开加密密钥 KPcard(1)解密并抽出（步骤 S124）.

接下来，分发控制部 312 以分发信息数据库 304 等所保存的数据为基础，生成含有许可 ID 数据等的许可信息数据 License（步骤 S126）.

进而，音乐服务器 30 从分发信息数据库 304 获得加密内容数据[Dc]Kc 并通过通信装置 350 发送给存储插件 110（步骤 S128）.

便携式电话机 100 接收数据[Dc]Kc 后（步骤 S130），在存储插件 110 中将接收到的数据[Dc]Kc 直接存放于存储器 1412 中（步骤 S132）.

另一方面，音乐服务器 30 从分发信息数据库 304 获得许可 Key Kc（步骤 S134），加密处理部 320 根据解密处理部 318 所提供的公开加密密钥 KPcard(1)对来自分发控制部 312 的许可 Key Kc 和许可信息数据 License 进行加密处理（步骤 S136）.

加密处理部 322 收到由加密处理部 320 所加密的数据[Kc, License]Kcard(1)，再将根据对话 Key Ks 加密的数据提供给数据总线 BS1. 通信装置 350 将加密处理部 322 所加密的数据[[Kc, License]Kcard(1)]Ks 发送给存储插件 110.

便携式电话机 100 接收数据[[Kc, License]Kcard(1)]Ks 后（步骤 S142），在存储插件 110 中解密处理部 1410 根据对话 Key Ks 进行解密处理，抽出数据[Kc, License]Kcard(1)并记录（存放）于存储器 1412 中（步骤 S146）.

进而，在存储插件 110 中，在控制器 1420 的控制下，解密处理部 1416 对存放于存储器 1412 中的数据[Kc, License]Kcard(1)进行解密，并将解密后的许可信息数据 License 存放于寄存器 1500 中（步骤

148）。

根据以上的动作，存储插件本身在将公开加密密钥 KPmedia(1)发送至对话 Key Ks 的发送侧（音乐服务器 30）之后可以接受分发，存储插件 110 中存放的内容数据成为可再生的状态。以下将存储插件中存放的内容数据成为可再生的状态称作“存储插件 110 处于状态 SA”。另一方面，将存储插件中存放的内容数据成为不能再生的状态称作“存储插件 110 处于状态 SB”。

进而，存储插件 110 向音乐服务器 30 发出分发受理通知，音乐服务器 30 接收分发受理后（步骤 S150），用户 1 的收费数据被存放于收费数据库 302（步骤 S152），处理结束（步骤 S154）。

图 8 为用以说明在便携式电话机 100 内，从存储插件 110 所保存的加密内容数据中对内容数据进行解密并作为音乐输出至外部的再生处理的流程图。

参照图 8，根据来自便携式电话机 100 的接触 Key 部 1108 等的用户 1 的指示，向存储插件 110 输出再生请求（步骤 S200）。

在存储插件 110 中，对应该再生请求，控制器 1420，根据寄存器 1500 所保存的许可信息数据 License 判断是否为可再生数据的请求（步骤 S202），当判断为可再生时，从 KPmedia(1)保存部 1401 向便携式电话机 100 发送公开加密密钥 KPmedia(1)（步骤 S204）。另一方面，当判断为不能再生时，结束处理（步骤 S230）。

当判断为可再生并由存储插件 110 发送了公开加密密钥 KPmedia(1)时，在便携式电话机 100 中接收来自存储插件 110 的公开加密密钥 KPmedia(1)（步骤 S206），在 Ks 发生部 1502 生成对话 Key Ks，加密处理部 1504 根据公开加密密钥 KPmedia(1)将对话 Key Ks 加密生成加密对话 Key[Ks]KPmedia(1)，并通过数据总线 BS2 发送给存储插件 110（步骤 S208）。

通过数据总线 BS2，存储插件 110 收到由便携式电话机 100 生成的且已加密的对话 Key Ks，并根据秘密解密密钥 Kmedia(1)进行解密，抽出对话 Key Ks（步骤 S210）。

接下来，存储插件 110 从存储器 1412 中读出被加密的数据[Kc, License]Kcard(1)，解密处理部 1416 进行解密处理（步骤 S212）。

根据秘密解密密钥 Kcard(1)可将从存储器 1412 中读出的数据解

密时（步骤 S214），许可 Key Kc 被抽出（步骤 S216）。另一方面，在不能再生时，结束处理（步骤 S232）。

在从存储器 1412 中读出的数据可再生时（步骤 S214），在寄存器 1500 内的许可信息数据 License 中，关于再生次数的数据将被更改（步骤 S218）。

接下来，根据抽出的对话 Key Ks 将许可 Key Kc 加密（步骤 S220），并将已加密的许可 Key[Kc]Ks 提供给数据总线 BS2（步骤 S222）。

便携式电话机 100 的解密处理部 1506 根据对话 Key Ks 进行解密处理，据此获得许可 Key Kc（步骤 S224）。

接下来，存储插件 110 从存储器 1412 中读出加密内容数据[Dc]Kc 并提供给数据总线 BS2（步骤 S226）。

便携式电话机 100 的音乐再生部 1508 根据所抽出的许可 Key Kc 对加密内容数据[Dc]Kc 进行解密处理生成普通文的音乐数据（步骤 S228），并再生音乐信号提供给混合部 1510（步骤 S230）。数模转换部 1512 收到来自混合部 1510 的数据后进行转换，并向外部输出所再生的音乐，处理结束（步骤 S232）。

通过形成这样的结构，存储插件本身可以向对话 Key Ks 的发送侧（便携式电话机 100）发送公开加密密钥 KPmedia (1)，在此之上进行再生动作。

图 9 及图 10 为用以说明在两个存储插件之间进行音乐数据和 Key 数据等的移动或复制处理的第 1 及第 2 流程图。

首先设便携式电话机 102 为发送侧，便携式电话机 100 为接收侧。另外，设便携式电话机 102 中也装载有具有与存储插件 110 相同结构的存储插件 112。

便携式电话机 102 首先向本身一方的存储插件 112 及便携式电话机 100 输出移动请求或复制请求（步骤 S300）。

存储插件 112 对应该请求读出存储器 1412 内的加密内容数据[Dc]Kc 并输出至存储插件 110（步骤 S302），另一方面，便携式电话机 100 从便携式电话机 102 接收请求（步骤 S301），存储插件 110 将加密内容数据[Dc]Kc 存放于存储器 1412 中（步骤 S304）。

接下来，在便携式电话机 102 及 100 中，判断在步骤 S300 所提供的请求是“移动请求”还是“复制请求”（步骤 S306、步骤 S306 ），

当为“移动请求”时，存储插件 112 向便携式电话机 102 发送公开加密密钥 KPmedia(2)（步骤 S308），便携式电话机 102 接收公开加密密钥 KPmedia(2)（步骤 S312）。另一方面，在为“移动请求”时，存储插件 110 向便携式电话机 100 输出公开加密密钥 KPmedia(1)（步骤 S308 ），便携式电话机 100 向便携式电话机 102 发送公开加密密钥 KPmedia(1)（步骤 S310）。

便携式电话机 102 接收公开加密密钥 KPmedia(1)及公开加密密钥 KPmedia(2)后（步骤 S312、步骤 S312 ），在便携式电话机 102 中，对话 Key 发生电路 1502 生成对话 Key Ks（步骤 S303），加密处理部 1504 用公开加密密钥 KPmedia(1)及公开加密密钥 KPmedia(2)将对话 Key Ks 加密（步骤 S314）。

便携式电话机 102 通过数据总线 BS2 向存储插件 112 传送加密对话 Key[Ks]KPmedia(2)，在存储插件 112 中根据秘密解密密钥 Kmedia(2)解密并抽出对话 Key Ks（步骤 S328）。

进而，便携式电话机 102 向便携式电话机 100 发送加密对话 Key[Ks]KPmedia(1)（步骤 S316）。便携式电话机 100 接收加密对话 Key[Ks]KPmedia(1)后（步骤 S318），传送给存储插件 110，存储插件 110 的解密处理部 1404 进行解密，受理对话 Key Ks（步骤 S320）。

在存储插件 110 中，根据对话 Key Ks 将存储插件 110 的公开加密密钥 KPcard(1)加密（步骤 S322），并从便携式电话机 100 向便携式电话机 102 发送加密后的数据[KPcard(1)]Ks（步骤 S324）。便携式电话机 102 接收数据[KPcard(1)]Ks（步骤 S326），且存储插件 112 的对话 Key Ks 的受理完毕后（步骤 S328），在存储插件 112 中，根据对话 Key Ks 将从存储插件 110 所发送的加密数据[KPcard(1)]Ks 解密，并将存储插件 110 的公开加密密钥 KPcard(1)解密并抽出（步骤 S330）。

接下来，在存储插件 112 中，从存储器 1412 中读出根据存储插件 112 的公开加密密钥 KPcard(2)加密后的许可 Key Kc、许可信息数据 License（步骤 S332）。

接下来，存储插件 112 的解密处理部 1416 根据秘密解密密钥 Kcard(2)对许可 Key Kc、许可信息数据 License 进行解密处理（步骤 S334）。

存储插件 112 的控制器 1420 将经过如此解密后的许可信息数据 License 的值与寄存器 1500 内的数据值进行置换（步骤 S336）。

进而，存储插件 112 的加密处理部 1414 根据在解密处理部 1410 所抽出的存储插件 110 的公开加密密钥 KPcard(1)将许可 Key Kc、许可信息数据 License 加密（步骤 S338）。

由存储插件 112 的加密处理部 1414 所加密的数据通过切换开关 1408（接点 Pc 闭合）再提供给加密处理部 1406，加密处理部 1406 根据对话 Key Ks 将数据[Kc, License]Kcard(1)加密并生成数据[[Kc, License]Kcard(1)]Ks（步骤 S340）。

接下来，存储插件 112 向便携式电话机 102 输出数据[[Kc, License]Kcard(1)]Ks（步骤 S342），便携式电话机 102 向便携式电话机 100 发送数据[[Kc, License]Kcard(1)]Ks（步骤 S344）。

便携式电话机 100 接收到的数据[[Kc, License]Kcard(1)]Ks（步骤 S346）被传送给存储插件 110，存储插件 110 的解密处理部 1410 将加密后的数据[[Kc, License]Kcard(1)]Ks 解密，受理数据[Kc, License]Kcard(1)（步骤 S348）。

在存储插件 110 中，将由解密处理部 1410 根据对话 Key Ks 进行解密处理后的数据记录于存储器 1412（步骤 S350）。进而，在存储插件 110 中，解密处理部 1416 根据秘密解密密钥 Kcard(1)将数据[Kc, License]Kcard(1)解密，并将解密后的许可信息数据 License 存放于寄存器 1500（步骤 S352）。

已解密的许可信息数据 License 向寄存器 1500 的存放结束后，存储插件 110 向便携式电话机 100 发出移动受理通知，便携式电话机 100 向便携式电话机 102 发送移动受理（步骤 S354）。

便携式电话机 102 接收来自便携式电话机 100 的移动受理后，将其传递给存储插件 112，与此对应存储插件 112 删除寄存器 1500 中所存放的许可信息数据 License（步骤 S358）。

另一方面，便携式电话机 102 对应移动受理的接收，在显示器 1110 上显示向用户 2 询问是否可以删除与存储插件 112 的存储器 1412 内所存放的移动数据相对应的记忆数据的提示。与此对应，用户 2 从接触 Key1108 输入对该提示的回答（步骤 S360）。

寄存器 1500 内的数据删除完毕（步骤 S358），并且输入对上述

提示的回答后（步骤 S360），存储插件 112 内的控制器 1420 判断是否进行存储器 1412 内数据的删除（步骤 S362）。

当得到删除存储器 1412 内的该数据的指示时（步骤 S362），在控制器 1420 的控制下，存储器 1412 内的加密内容数据[Dc]Kc 及数据[Kc, License]kcard(2)被删除（步骤 S364），处理结束（步骤 S374）。

另一方面，当未得到删除存储器 1412 内的该数据的指示时（步骤 S362），处理结束（步骤 S374）。这种情况下，加密内容数据[Dc]Kc 及数据[Kc, License]Kcard(2)留在存储器 1412 中，但寄存器 1500 内不存在许可信息数据 License，所以用户 2 只要不再次请求从音乐服务器 30 分发再生信息，就不能再生音乐数据。即，存储插件 112 成为“状态 SB”。在存储插件 110 中，除了加密内容数据之外，还移动了许可 Key Kc、许可信息数据，所以存储插件 110 成为“状态 SA”。

另一方面，在步骤 S306’，当判断为提供有“复制请求”时，从便携式电话机 100 向便携式电话机 102 发送复制受理（步骤 S370）。在便携式电话机 102 中，接收复制受理后（步骤 S372），处理结束（步骤 S374）。

通过形成如此结构，存储插件本身可以向对话 Key Ks 的发送侧（便携式电话机 100）发送公开加密密钥 KPmedia(1)及 KPmedia(2)，在此之上进行移动动作及复制动作。

[实施方式 2]

在实施方式 2 的数据分发系统中，与实施方式 1 的数据分发系统的结构不同，其以形成如下结构为其特征之一：分发服务器、便携式电话机及存储插件分别生成各自的对话 Key。即，将分发服务器或便携式电话机产生的对话 Key 作为对话 Key Ks，将一方的存储插件 120 产生的对话 Key 作为对话 Key Ks1，将具有与存储插件 120 相同结构的另一方的存储插件 122 产生的对话 Key 作为对话 Key Ks2。

即，在实施方式 2 的数据分发系统中以形成如下结构为其特征之一：构成系统的各个设备本身生成对话 Key，在收到数据时，换句话说就是在其成为数据的接收方时，首先向对方（发送方）分发对话 Key。发送方用从该接收方所分发的对话 Key 将数据加密，并发送该加密数据。接收方则根据本身生成的对话 Key 将收到的数据解密。

另外，为了实现如上动作，在再生动作中，便携式电话机侧将用

于收到存储插件所生成的对话 Key 的公开加密密钥作为 KPp，将能够对以该公开加密密钥 KPp 加密的数据进行解密的秘密解密密钥作为密钥 Kp.

图 11 为表示对应于实施方式 2 的存储插件 120 的分发服务器 11 的结构的概略框图. 其与图 3 所示分发服务器 10 的结构的不同之处为：数据处理部 310 的加密处理部 322 不是根据来自 Ks 发生部 314 的对话 Key Ks，而是根据由便携式电话机所装载的存储插件用对话 Key Ks1、Ks2 加密并发送、由解密处理部 318 解密并抽出的对话 Key，例如根据对话 Key Ks1，对加密处理部 320 的输出再行加密，并通过数据总线 BS1 提供给通信装置 350.

分发服务器 11 的其他各处与图 3 所示实施方式 1 的分发服务器 10 的结构相同，所以对同一部分赋予同一符号，不再重复其说明.

图 12 为用以说明实施方式 2 的便携式电话机 101 的结构的概略框图.

其与图 4 所示便携式电话机 100 的结构的不同之处为：首先，除其装载有存储插件 120 之外，便携式电话机 101 还具备保存公开加密密钥 KPp 并在再生动作时向数据总线 BS2 输出公开加密密钥 KPp 的 KPp 保存部 1524.

其次，便携式电话机 101 还具备保存秘密解密密钥 Kp 的 Kp 保存部 1520 以及根据该 Kp 保存部 1520 所提供的秘密解密密钥 Kp 将以存储插件 120 通过数据总线 BS2 提供的公开加密密钥 KPp 加密的对话 Key Ks1 解密并抽出的解密处理部 1552. 而且，加密处理部 1504 根据该解密处理部 1522 所提供的对话 Key Ks1 将来自 Ks 发生部 1502 的本身的对话 Key Ks 加密并输出给数据总线 BS2.

便携式电话机 101 的其他各处与图 4 所示实施方式 1 的便携式电话机 100 的结构相同，所以对同一部分赋予同一符号，不再重复其说明.

图 13 为用以说明本发明的实施方式 2 的存储插件 120 的结构的概略框图，同时是实施方式 1 的图 5 的对比图.

存储插件 120 的结构与存储插件 110 的结构的不同之处为：首先，存储插件 120 具备产生该插件单独的对话 Key Ks1 的对话 Key Ks1 发生部 1432.

其次，存储插件 120 还具备用以将对话 Key 发生电路 1432 所生成的对话 Key Ks1 加密并提供给数据总线 BS3 的加密处理部 1430。

与此对应，存储插件 120 还具备：在再生模式中接受并保存形态电话机 101 的公开加密密钥 KPp 的 KPp 受理部 1407；在移动模式中接受并保存对方（移动目标）的公开加密密钥 KPmedia(n) 的 KPmedia 受理部 1403；接受该 KPmedia 受理部 1403 的输出和 KPp 受理部 1407 的输出，并对应动作模式输出其中某一方的切换开关 1436。切换开关 1436 具有接点 Pi 及 Ph，接点 Pi 与 KPp 受理部 1407、接点 Ph 与 KPmedia 受理部 1403 分别联结。加密处理部 1430 根据切换开关 1436 所提供的公开加密密钥 KPmedia(n) 或公开加密密钥 KPp 的二者之一将来自 Ks1 发生部 1432 的对话 Key Ks1 加密并提供给数据总线 BS3。

即，切换开关 1436 在分发动作时以及在移动动作中为移动目标时其为未使用状态，在再生动作时在接点 Pi 侧闭合，在移动动作中为移动源时在接点 Ph 侧闭合。

存储插件 120 还具备切换开关 1435，其具有接点 Pe、Pf 及 Pg，接受从解密处理部 1404 所提供的来自音乐服务器的对话 Key Ks、Ks1 发生部 1432 的输出、从数据总线 BS4 所提供的来自便携式电话机 101 的对话 Key Ks 并对应动作模式有选择地输出其中某一方。来自解密处理部 1404 的输出、Ks1 发生部 1432 的输出、数据总线 BS4 分别联结于接点 Pe、接点 Pf、接点 Pg。因此，加密处理部 1406 和解密处理部 1410 根据从该切换开关 1435 所提供的 Key 分别进行加密处理及解密处理。

即，切换开关 1435 在分发动作中进行来自音乐服务器 31 的对话 Key Ks1 的抽出时在接点 Pe 侧闭合；在分发动作中根据对话 Key Ks1 就来自音乐服务器 31 的加密许可 Key Kc、许可信息数据进行解密时在接点 Pf 侧闭合。切换开关 1435 在再生动作中进行解密处理时在接点 Pf 侧闭合；在再生动作中进行加密处理时在接点 Pg 侧闭合。切换开关 1435 在移动动作中为移动源且进行解密处理时在接点 Pf 侧闭合；在移动动作中为移动源且进行加密处理时在接点 Pg 侧闭合。切换开关 1435 在移动动作中为移动目标且收到移动源的对话 Key 时在接点 Pe 侧闭合；在移动动作中为移动目标且收到许可 Key Kc 及许可信息数据 License 时在接点 Pf 侧闭合。

存储插件 120 还具备代替切换开关 1408 的切换开关 1409，其具有接点 Pa、Pb、Pc 及 Pd，接受从 Ks1 发生部 1432 所提供的本身的对话 Key Ks1、KPcard 保存部 1405 的输出、从数据总线 BS5 所提供的许可 Key Kc、从加密处理部 1414 所提供的根据对方的公开加密密钥 KPcard(n)加密后的许可 Key Kc 及许可信息数据 License 并对应动作模式有选择地输出其中某一方。

来自 Ks1 发生部 1432 的输出、KPcard(1)保存部 1405 的输出、数据总线 BS5、加密处理部 1414 的输出分别联结于接点 Pa、接点 Pb、接点 Pc、接点 Pd。因此，加密处理部 1406 对从该切换开关 1409 所提供的数据分别进行加密处理。

即，切换开关 1409 在分发模式中为分发目标且向音乐服务器 31 发送本身的公开加密密钥 KPcard(1)和本身的对话 Key Ks1 时，依次在接点 Pb 侧及接点 Pa 侧闭合。切换开关 1409 在再生模式时，在接点 Pc 侧闭合；在移动模式中为移动源时在接点 Pd 侧闭合。切换开关 1409 在移动模式中为移动目标且向移动源发送本身的公开加密密钥 KPcard(1)和本身的对话 Key Ks1 时，也依次在接点 Pb 侧及接点 Pa 侧闭合。

图 14 及图 15 为用以说明采用了在图 13 说明的存储插件 120 的分发模式的第 1 及第 2 流程图。

在图 14 及图 15 中也对用户 1 通过使用存储插件 120 从音乐服务器 31 接受音乐数据的分发的分发模式的动作进行说明。

首先，由用户通过对接触 Key1108 的按密钥操作等从用户 1 的便携式电话机 101 发出分发请求（步骤 S100）。

在存储插件 120 中，对应该分发请求将公开加密密钥 KPmedia(1)从 KPmedia(1)保存部 1401 发送给音乐服务器 31（步骤 S102）。进而，在存储插件 120 中由 Ks1 发生部 1432 生成对话 Key Ks1（步骤 S109）。

在音乐服务器 31 中接收从存储插件 120 所传递的分发请求及公开加密密钥 KPmedia(1)时（步骤 S104），根据接收到的公开加密密钥 KPmedia(1)向认证服务器 12 进行查询，当为采用了正规存储插件的访问时移交下一步处理（步骤 S106），当为非正规存储插件时结束处理（步骤 S154）。

查询的结果，当确认为正规存储插件时，在音乐服务器 31 中，对

话 Key 发生部 314 生成对话 Key Ks. 进而，音乐服务器 31 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1)将该对话 Key Ks 加密并生成加密对话 Key[Ks]Kmedia(1)（步骤 S108）.

接下来，音乐服务器 31 将加密对话 Key[Ks]Kmedia(1)提供给数据总线 BS1. 通信装置 350 通过通信网向便携式电话机 101 的存储插件 120 发送来自加密处理部 316 的加密对话 Key[Ks]Kmedia(1)（步骤 S110）.

便携式电话机 101 接收加密对话 Key[Ks]Kmedia(1)后（步骤 S112），在存储插件 120 中，解密处理部 1404 用秘密解密密钥 Kmedia(1)对通过存储器接口 1200 提供给数据总线 BS3 的接收数据进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S114）.

接下来，在分发模式中，切换开关 1409 的接点 Pa 或 Pb 选择依次闭合状态，所以加密处理部 1406 根据对话 Key Ks 对通过接点 Pa 从对话 Key 发生部 1432 所提供的对话 Key Ks1 和通过接点 Pb 从 KPcard(1)保存部 1405 所提供的公开加密密钥 KPcard(1)（对于存储插件 120 的公开加密密钥）进行加密（步骤 S116），生成数据[KPcard(1)、Ks1]Ks（步骤 S118）.

便携式电话机 101 将由加密处理部 1406 所加密的数据[KPcard(1)、Ks1]Ks 发送给音乐服务器 31（步骤 S120）.

在音乐服务器 31 中，由通信装置 350 接收数据[KPcard(1)、Ks1]Ks（步骤 S122），解密处理部 318 根据对话 Key Ks 对提供给数据总线 BS1 的数据[KPcard(1)、Ks1]Ks 进行解密处理，将公开加密密钥 KPcard(1)及对话 Key Ks1 解密并抽出（步骤 S124）.

接下来，分发控制部 312 以分发信息数据库 304 等所保存的数据为基础，生成含有许可 ID 数据等的许可信息数据 License（步骤 S126）.

进而，音乐服务器 31 从分发信息数据库 304 获得加密内容数据[Dc]Kc 并通过通信装置 350 发送给存储插件 120（步骤 S128）.

便携式电话机 101 接收加密内容数据[Dc]Kc 后（步骤 S130），在存储插件 120 中将接收到的加密内容数据[Dc]Kc 直接存放于存储器 1412 中（步骤 S132）.

另一方面，音乐服务器 31 从分发信息数据库 304 获得许可 Key Kc

（步骤 S134），加密处理部 320 根据解密处理部 318 所提供的公开加密密钥 KPcard(1)对来自分发控制部 312 的许可 Key Kc 和许可信息数据 License 进行加密处理（步骤 S136）。

加密处理部 322 收到由加密处理部 320 所加密的数据[Kc，License]Kcard(1)，再将根据来自存储插件 120 的对话 Key Ks1 加密的数据提供给数据总线 BS1。通信装置 350 将加密处理部 322 所加密的数据[[Kc，License]Kcard(1)]Ks1 发送给存储插件 120。

便携式电话机 101 接收数据[[Kc，License]Kcard(1)]Ks1 后（步骤 S142），在存储插件 120 中解密处理部 1410 根据由 Ks1 发生部 1432 通过接点 Pf 提供的对话 Key Ks1 进行解密处理，抽出数据[Kc，License]Kcard(1)并存放于存储器 1412 中（步骤 S146）。

进而，在存储插件 120 中，在控制器 1420 的控制下，解密处理部 1416 对存放于存储器 1412 中的数据[Kc，License]Kcard(1)进行解密，并将解密后的许可信息数据 License 存放于寄存器 1500 中（步骤 148）。

根据如上动作，存储插件 120 本身将公开加密密钥 KPmedia(1)及对话 Key Ks1 发送给加密内容数据的发送侧（音乐服务器 31）之后，可以接受分发，存储插件 120 成为可再生音乐信息的状态。

进而，存储插件 120 向音乐服务器 31 发出分发受理通知，音乐服务器 31 接收分发受理后（步骤 S150），用户 1 的收费数据被存放于收费数据库 302（步骤 S152），处理结束（步骤 S154）。

图 16 及图 17 为用以说明在便携式电话机 101 内从存储插件 120 所保存的加密内容数据中对音乐数据的内容数据进行解密并作为音乐数据输出至外部的再生模式的第 1 及第 2 流程图。

参照图 16 及图 17，根据来自便携式电话机的接触 Key1108 等的用户 1 的指示，向存储插件 120 输出再生请求（步骤 S200）。

在存储插件 120 中，对应该再生请求，控制器 1420 根据寄存器 1500 所保存的许可信息数据 License 判断是否为可解密数据的请求（步骤 S202），当判断为可再生时，向便携式电话机 101 发送可再生通知（步骤 S240）。另一方面，当判断为不能再生时结束处理（步骤 S280）。

当判断为可再生并由存储插件 120 发送了可再生通知时，在便携式电话机 101 中将公开加密密钥 KPp 发送给存储插件 120（步骤

S242），在 Ks 发生部 1502 生成对话 Key Ks（步骤 S244）。

另一方面，存储插件 120 也生成对话 Key Ks1（步骤 S240）。存储插件 120 进而根据通过数据总线 BS2 从便携式电话机 101 收得的公开加密密钥 KPp 将对话 Key Ks1 加密（步骤 S248），并将生成的加密对话 Key[Ks1]Kp 发送给便携式电话机 101（步骤 S250）。

在便携式电话机 101 中接收来自存储插件 120 的加密对话 Key[Ks1]Kp 后，解密处理部 1522 根据秘密解密密钥 Kp 进行解密并抽出由存储插件 120 生成的对话 Key Ks1（步骤 S252）。接下来，便携式电话机 101 的加密处理部 1504 根据对话 Key Ks1 将便携式电话机 101 所生成的对话 Key Ks 加密，生成加密对话 Key[Ks]Ks1（步骤 S254），并将该加密对话 Key[Ks]Ks1 发送给存储插件 120（步骤 S256）。

通过数据总线 BS2，存储插件 120 收到由便携式电话机 101 所生成的加密对话 Key[Ks]Ks1，并根据对话 Key Ks1 进行解密，抽出便携式电话机 101 所生成的对话 Key Ks（步骤 S258）。

接下来，存储插件 120 从存储器 1412 中读出被加密的数据[Kc, License]Kcard(1)，解密处理部 1416 进行解密处理（步骤 S260）。

根据秘密解密密钥 Kcard(1)可将从存储器 1412 中读出的数据解密时（步骤 S262），许可 Key Kc 被抽出（步骤 S264）。另一方面，在不能解密时结束处理（步骤 S280）。

当从存储器 1412 所读出的数据可被解密时，进而在寄存器 1500 内的许可信息数据 License 中，有关再生次数的数据将被更改（步骤 S266）。

接下来，在存储插件 120 中，加密处理部 1406 根据抽出的对话 Key Ks 将许可 Key Kc 加密（步骤 S268），并将加密许可 Key[Kc]Ks 提供给数据总线 BS2（步骤 S270）。

便携式电话机 101 的解密处理部 1506 根据对话 Key Ks 进行解密处理，据此获得许可 Key Kc（步骤 S272）。

接下来，存储插件 120 从存储器 1412 中读出加密内容数据[Dc]Kc 并提供给数据总线 BS2（步骤 S274）。

便携式电话机 101 的音乐再生部 1508 根据所抽出的许可 Key Kc 对加密内容数据[Dc]Kc 进行解密处理生成普通文的内容数据（步骤

S276），并再生音乐信号提供给混合部 1510（步骤 S276）。数模转换部 1512 收到来自混合部 1510 的音乐信号后进行转换，并向外部输出所再生的音乐，处理结束（步骤 S232）。

通过形成这样的结构，存储插件本身及携带电话本身可以分别生成对话 Key Ks1 或 Ks 并对据此加密的数据进行交换，在此之上进行再生动作。

图 18 及图 19 为用以说明在两个存储插件之间进行内容数据及 Key 数据等的移动模式或复制模式的处理的第 1 及第 2 流程图。

首先设具有与便携式电话机 101 相同结构的便携式电话机 103 为发送侧，便携式电话机 101 为接收侧。另外，设便携式电话机 103 中也装载有具有与存储插件 120 相同结构的存储插件 122。

便携式电话机 103 首先向本身一方的存储插件 122 及便携式电话机 101 输出移动请求或复制请求（步骤 S300）。

存储插件 122 对应该请求读出存储器 1412 内的加密内容数据 [Dc]Kc 并输出至存储插件 120（步骤 S302），另一方面，便携式电话机 101 接收来自便携式电话机 103 的请求（步骤 S301），存储插件 120 将加密内容数据 [Dc]Kc 存放于存储器 1412 中（步骤 S304）。

接下来，在便携式电话机 103 及 101 中，判断在步骤 S300 所提供的请求是“移动请求”还是“复制请求”（步骤 S306、步骤 S306 ），当为“移动请求”时，存储插件 120 向便携式电话机 101 输出公开加密密钥 KPmedia(1)（步骤 S308），便携式电话机 101 向便携式电话机 103 发送公开加密密钥 KPmedia(1)（步骤 S310）。

便携式电话机 103 接收公开加密密钥 KPmedia(1)（步骤 S312）并传递给存储插件 122 后（步骤 S313），存储插件 122 的 Ks2 发生电路 1432 生成对话 Key Ks2（步骤 S314），加密处理部 1430 用公开加密密钥 KPmedia(1) 将对话 Key Ks2 加密（步骤 S315）。

便携式电话机 103 向便携式电话机 101 发送加密对话 Key[Ks2]KPmedia(1) （步骤 S316）。便携式电话机 101 接收加密对话 Key[Ks2]KPmedia(1) 后（步骤 S318），传送给存储插件 120，存储插件 120 的解密处理部 1404 进行解密，受理对话 Key Ks2，进而在对话 Key 生成部 1432 生成存储插件 120 的对话 Key Ks1（步骤 S320）。

在存储插件 120 中，根据对话 Key Ks2 将存储插件 120 的公开加

密密钥 KPcard(1)及对话 Key Ks1 加密（步骤 S322），并从便携式电话机 101 向便携式电话机 103 发送加密后的数据[KPcard(1)、Ks1]Ks2（步骤 S324）。便携式电话机 103 接收数据[KPcard(1)、Ks1]Ks2（步骤 S326），并传递给存储插件 122。

在存储插件 122 中解密处理部 1410 根据对话 Key Ks2 将从存储插件 120 所发送的加密数据[KPcard(1)、Ks1]Ks2 解密，并将存储插件 120 的公开加密密钥 KPcard(1)、对话 Key Ks1 解密并抽出（步骤 S330）。

接下来，在存储插件 122 中，从存储器 1412 中读出根据存储插件 122 的公开加密密钥 KPcard(2)加密后的许可 Key Kc、许可信息数据 License 所对应的[Kc, License]Kcard(2)（步骤 S332）。

接下来，存储插件 122 的解密处理部 1416 根据秘密解密密钥 Kcard(2)对[Kc, License]Kcard(2)进行解密处理（步骤 S334）。

存储插件 122 的控制器 1420 将经过如此解密后的许可信息数据 License 的值与寄存器 1500 内的数据值进行置换（步骤 S336）。

进而，存储插件 122 的加密处理部 1414 根据在解密处理部 1410 所抽出的存储插件 120 的公开加密密钥 KPcard(1)将许可 Key Kc、许可信息数据 License 加密（步骤 S338）。

由存储插件 122 的加密处理部 1414 所加密的数据通过切换开关 1409（接点 Pd 闭合）再提供给加密处理部 1406，存储插件 122 的加密处理部 1406 根据对话 Key Ks1 将数据[Kc, License]Kcard(1)加密并生成数据[[Kc, License]Kcard(1)]Ks1（步骤 S340）。

接下来，存储插件 122 向便携式电话机 103 输出数据[[Kc, License]Kcard(1)]Ks1 （步骤 S342），便携式电话机 103 向便携式电话机 101 发送数据[[Kc, License]Kcard(1)]Ks1（步骤 S344）。

便携式电话机 101 接收到的数据[[Kc,License]Kcard(1)]Ks1（步骤 S346）被传送给存储插件 120，存储插件 120 的解密处理部 1410 将加密后的数据[[Kc, License]Kcard(1)]Ks1 解密，受理数据[Kc, License]Kcard(1)（步骤 S348）。

在存储插件 120 中，将由解密处理部 1410 根据对话 Key Ks1 进行解密处理后的数据[Kc, License]Kcard(1)存放于存储器 1412（步骤 S350）。进而，在存储插件 120 中，解密处理部 1416 根据秘密解密密

钥 Kcard(1)将数据 [Kc，License]Kcard(1)解密，并将解密后的许可信息数据License存放于寄存器1500（步骤S352）。

以后的移动模式中的处理以及复制模式中存储插件120和122的处理与以图9及图10说明的实施方式1的存储插件110、112等的处理相同，因此不再重复其说明。

通过形成如此结构，移动源及移动目标的存储插件本身可以分别生成对话Key，在此之上施行移动模式。

因而，对数据总线上等所传送的数据的许可Key Kc及许可信息数据License进行加密的密钥按各对话且按各设备变更，所以有进一步提高许可Key Kc及许可信息数据License的交换的安全性这一效果。

而且，通过采用如上结构，有进一步提高用户的便利性这一效果，例如可以不通过具有如上所述的对话Key发生电路1502的便携式电话机终端，而凭借可连接存储插件与存储插件的接口设备进行从存储插件122向存储插件120的数据的移动。

在此，在移动时，关于限制再生次数的许可信息数据内的设定，通过将存储器1412中记录的许可信息数据变更为记录有每次在寄存器1500中再生时所修正的再生次数的许可信息数据而更新许可信息数据。这样，即使在存储插件之间移动内容数据，也可以使有再生次数限制的内容数据的再生次数不会超过分发时所决定的再生次数的限制。

[实施方式3]

在实施方式3的数据分发系统中以形成如下结构为其特征之一：用户不是从分发媒体——便携式电话机公司接受加密内容数据的分发，而是从例如设置于街头等的内容数据销售机接受加密内容数据的供给。

图20为用于说明如此实施方式3的数据分发系统的结构的概念图。另外，便携式电话机100及存储插件110的结构与实施方式1中说明的相同，所以不再重复其说明。

参照图20，内容数据销售机2000具备向用户输出分发作业引导等用的显示器2002、用户输入指示用密钥盘2004、费用投入口2006、通过便携式电话机100和插接件1120进行数据交换用的外部插接件2010。内容数据销售机2000还通过便携式电话网等的通信路与管理销

售记录等用的管理服务器2200相连接。

图21为表示实施方式3的内容数据销售机2000的结构的概略框图。如上所述，内容数据销售机2000具备：显示器2002；密钥盘2004；费用受理部2020，接受来自费用投入口2006的投入金；外部插接件2010；接口部2012，设于插接件2010与数据总线之间；分发信息数据库304，用以保存按照规定的方式将内容数据（音乐数据）加密后的数据和许可信息数据等分发信息；通信装置360，用以与管理服务器2200之间进行信息交换；数据处理部2100，通过数据总线BS1收到来自分发信息数据库304及管理服务器2200的数据并进行规定的加密处理。

与实施方式1相同，数据处理部2100中包括：分发控制部312，用以对应数据总线BS1上的数据，对数据处理部2100的动作进行控制；对话Key发生部314，用以在分发控制部312的控制下产生对话Key Ks；加密处理部316，用以根据插件媒体固有的公开加密密钥KPmedia(n)将对话Key发生部314所生成的对话Key Ks加密并提供给数据总线BS1；解密处理部318，通过数据总线BS1接受在各用户的便携式电话机中根据对话Key Ks加密后从插接件2010所提供的数据并进行解密处理；加密处理部320，使用由解密处理部318所抽出的公开加密密钥KPcard(n)，用以在分发控制部312的控制下对许可信息数据进行加密；加密处理部322，根据对话Key Ks对加密处理部320的输出再行加密，并通过数据总线BS1提供给插接件2010。

图22及图23为用以说明以图20及图21说明的数据分发系统的分发模式的第1及第2流程图。

在图22及图23中，对用户1通过使用存储插件110从内容数据销售机2000接受音乐数据的分发时的动作进行说明。

首先，用户凭借对内容数据销售机2000的密钥盘2004的按密钥操作等发出分发请求的指示（步骤S400）。内容数据销售机2000向存储插件110输出公开加密密钥KPmedia(1)的发送要求（步骤S402）。

在存储插件110中，对应该公开加密密钥KPmedia(1)的发送要求，从KPmedia(1)保存部1401向便携式电话机100输出公开加密密钥KPmedia(1)（步骤S406）。

便携式电话机 100 向内容数据销售机 2000 发送公开加密密钥 KPmedia(1)（步骤 S408），内容数据销售机 2000 接收从存储插件 110 所传递的公开加密密钥 KPmedia(1)后（步骤 S410）通过显示器 2002 引导用户投入费用，并收取费用（步骤 S412）。接下来，内容数据销售机 2000 的对话 Key 发生部 314 生成对话 Key Ks。进而，内容数据销售机 2000 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1)将该对话 Key Ks 加密并生成加密对话 Key[Ks]Kmedia(1)（步骤 S414）。

接下来，内容数据销售机 2000 将加密对话 Key[Ks]Kmedia(1)提供给数据总线 BS1 并从插接件 2010 输出（步骤 S416）。便携式电话机 100 接收该加密对话 Key[Ks]Kmedia(1)后传递给存储插件 110（步骤 S418）。

在存储插件 110 中，解密处理部 1404 根据秘密解密密钥 Kmedia(1)对通过存储器接口 1200 提供给数据总线 BS3 的加密对话 Key[Ks]Kmedia(1)进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S420）。

接下来，在分发模式中，切换开关 1408 的接点 Pa 选择闭合状态，所以加密处理部 1406 根据对话 Key Ks 将通过接点 Pa 从 KPcard(1)保存部 1405 所提供的公开加密密钥 KPcard(1)加密（步骤 S422），生成数据[KPcard(1)]Ks（步骤 S424）。

便携式电话机 100 向内容数据销售机 2000 发送由加密处理部 1406 所加密的数据[KPcard(1)]Ks（步骤 S426）。

在内容数据销售机 2000 中，通过插接件 2010 接收数据[KPcard(1)]Ks（步骤 S428），解密处理部 318 根据对话 Key Ks 对提供给数据总线 BS1 的数据[KPcard(1)]Ks 进行解密处理，将公开加密密钥 KPcard(1)解密并抽出（步骤 S430）。

接下来，分发控制部 312 以分发信息数据库 304 等所保存的数据为基础生成包含许可 ID 数据等的许可信息数据 License(步骤 S432)。

进而，内容数据销售机 2000 从分发信息数据库 304 获得加密内容数据[Dc]Kc 并通过插接件 2010 发送给便携式电话机 100（步骤 S434）。

便携式电话机 100 接收加密内容数据[Dc]Kc 后（步骤 S436），在

存储插件 110 中将接收到的加密内容数据[Dc]Kc 直接存放于存储器 1412（步骤 S438）。

另一方面，内容数据销售机 2000 从分发信息数据库 304 获得许可 Key Kc（步骤 S440），加密处理部 320 根据由解密处理部 318 所提供的公开加密密钥 KPcard(1)对来自分发控制部 312 的许可 Key Kc 和许可信息数据 License 进行加密处理（步骤 S442）。

加密处理部 322 收到由加密处理部 320 所加密的数据[Kc，License]Kcard(1)，并将根据对话 Key Ks 再行加密后的数据提供给数据总线 BS1，由加密处理部 322 所加密的数据[[Kc，License]Kcard(1)]Ks 被发送给存储插件 110（步骤 S446）。

便携式电话机 100 接收数据[[Kc，License]Kcard(1)]Ks 后（步骤 S448），在存储插件 110 中，解密处理部 1410 根据对话 Key Ks 进行解密处理，抽出数据[Kc，License]Kcard(1)并存放于存储器 1412（步骤 S452）。

进而，在存储插件 110 中，在控制器 1420 的控制下，解密处理部 1416 将存储器 1412 所存放的数据[Kc，License]Kcard(1)解密，并将所解密的许可信息数据 License 存放于寄存器 1500（步骤 S458）。

通过如上动作，存储插件本身可以向对话 Key Ks 的发送侧（内容数据销售机 2000）发送公开加密密钥 KPmeida(1)，在此之上接受分发，并成为能够用存储插件 110 所存放的加密内容数据再生音乐的状态。

进而，从存储插件 110 向内容数据销售机 2000 通过便携式电话机 100 发出分发受理通知（步骤 S460），内容数据销售机 2000 接收分发受理后（步骤 S462）向管理服务器发送销售记录（步骤 S464），处理结束（步骤 S466）。

通过如上结构，用户可以较简便地接受已加密的音乐数据等的分发。

[实施方式 3 的变化例]

在实施方式 3 的数据分发系统中的结构为：存储插件 110 通过便携式电话机 100 从内容数据销售机 2000 接受加密内容数据的分发。

但是，在图 21 所示的内容数据销售机 2000 的结构中，如果形成设置用作与存储插件 110 之间的接口的存储槽以取代插接件 2010 的结

构，就能够无需通过便携式电话机 100 而使存储插件 110 与内容数据销售机 2000 直接进行数据的交换。

图 24 为表示如此实施方式 3 的变化例的内容数据销售机 2001 的结构的概念图。其与图 20 所示实施方式 3 的内容数据销售机 2000 的结构的不同之处在于其形成如下结构：取代外部插接件 2010，设置可以插入存储插件的插件槽 2030，该插件槽 2030 通过接口部 2010 与数据总线 BS1 进行数据交换。

图 25 及图 26 为用以说明实施方式 3 的变化例的数据分发系统的分发模式的第 1 及第 2 流程图。

除了存储插件 110 与内容数据销售机 2001 不通过便携式电话机 100 进行数据交换这一点之外，其与图 22 及图 23 所示实施方式 3 的分发模式的处理相同，所以对同一处理赋予同一符号，不再重复其说明。

通过如上结构及动作，用户可以更加简便地接受已加密的音乐数据等的分发。

而且具有这一优点：存储插件可以独立接受并存放加密内容数据的分发，所以进行内容数据的再生单元的选择范围增大，将进一步提高用户的便利性。

[实施方式 4]

图 27 为用以说明实施方式 4 的内容数据销售机 3000 的结构的概略框图。其与图 21 所示内容数据销售机 2000 的结构的不同之处为：成为对象的存储插件为实施方式 2 的存储插件 120，且所使用的终端为便携式电话机 101；以及与此对应，数据处理部 2100 的加密处理部 322 不是根据来自 Ks 发生部 314 的对话 Key Ks，而是根据从便携式电话机所装载的存储插件中凭借对话 Key Ks 加密后所发送的并由解密处理部 318 解密并抽出的对话 Key 例如对话 Key Ks1 对加密处理部 320 的输出再行加密，并通过数据总线 BS1 提供给接口部 2012 及插接件 2010。

内容数据销售机 3000 的其他各处与图 21 所示实施方式 3 的内容数据销售机 2000 的结构的结构相同，所以对同一部分赋予同一符号而不再重复其说明。

另外，便携式电话机 101 及存储插件 110 的结构也与实施方式 2 中说明的相同，所以也不重复其说明。

图 28 及图 29 为用以说明以图 27 说明的数据分发系统的分发模式的第 1 及第 2 流程图。

在图 28 及图 29 中，对用户 1 通过使用存储插件 120 从内容数据销售机 3000 接受音乐数据的分发时的动作进行说明。

首先，用户通过对内容数据销售机 3000 的密钥盘 2004 的按密钥操作发出分发请求指示（步骤 S500）。内容数据销售机 3000 向存储插件 110 输出公开加密密钥 KPmedia(1)的发送要求（步骤 S502）。

在存储插件 120 中，对应该公开加密密钥 KPmedia(1)的发送要求，从 KPmedia(1)保存部 1401 向内容数据销售机 3000 发送公开加密密钥 KPmedia(1)（步骤 S506）。进而，在存储插件 120 中，由 Ks1 发生部 1432 生成对话 Key Ks1（步骤 S515）。

便携式电话机 101 向内容数据销售机 3000 发送公开加密密钥 KPmedia(1)（步骤 S508），内容数据销售机 3000 接收从存储插件 120 所传递的公开加密密钥 KPmedia(1)后（步骤 S510），通过显示器 2002 引导用户投入费用，并收取费用（步骤 S512）。接下来，内容数据销售机 3000 的对话 Key 发生部 314 生成对话 Key Ks。进而，内容数据销售机 3000 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1)将该对话 Key Ks 加密生成加密对话 Key[Ks]Kmedia(1)（步骤 S514）。

接下来，内容数据销售机 3000 将加密对话 Key[Ks]Kmedia(1)提供给数据总线 BS1，并从插接件 2010 输出（步骤 S416）。便携式电话机 101 接收该加密对话 Key[Ks]Kmedia(1)后传递给存储插件 120（步骤 S518）。

在存储插件 120 中，解密处理部 1404 根据秘密解密密钥 KPmedia(1)对通过存储器接口 1200 提供给数据总线 BS3 的加密对话 Key[Ks]Kmedia(1)进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S520）。

接下来，加密处理部 1406 根据对话 Key Ks 将从 KPcard(1)保存部 1405 所提供的公开加密密钥 KPcard(1)以及来自 Ks1 发生部 1432 的对话 Key Ks1 加密（步骤 S522），生成数据[KPcard(1)、Ks1]Ks（步骤 S524）。

便携式电话机 101 将由加密处理部 1406 所加密的数据

[KPcard(1)、Ks1]Ks 发送给内容数据销售机 3000（步骤 S526）。

在内容数据销售机 3000 中，通过插接件 2010 接收数据[KPcard(1)、Ks1]Ks（步骤 S528），解密处理部 318 根据对话 Key Ks 对提供给数据总线 BS1 的数据[KPcard(1)、Ks1]Ks 进行解密处理，将公开加密密钥 KPcard(1)及对话 Key Ks1 解密并抽出（步骤 S530）。

接下来，分发控制部 312 以分发信息数据库 304 等所保存的数据为基础，生成含有许可 ID 数据等的许可信息数据 License（步骤 S532）。

进而，内容数据销售机 3000 从分发信息数据库 304 获得加密内容数据[Dc]Kc 并通过插接件 2010 发送给便携式电话机 101（步骤 S534）。

便携式电话机 101 接收加密内容数据[Dc]Kc 后（步骤 S536），在存储插件 120 中，将接收到的加密内容数据[Dc]Kc 直接存放于存储器 1412（步骤 S538）。

另一方面，内容数据销售机 3000 从分发信息数据库 304 获得许可 Key Kc（步骤 S540），加密处理部 320 根据由解密处理部 318 所提供的公开加密密钥 KPcard(1)对来自分发控制部 312 的许可 Key Kc 和许可信息数据 License 进行加密处理（步骤 S542）。

加密处理部 322 收到由加密处理部 320 所加密的数据[Kc、License]Kcard(1)，并将根据对话 Key Ks1 再行加密的数据提供给数据总线 BS1，由加密处理部 322 所加密的数据[[Kc，License]Kcard(1)]Ks1 被输出给便携式电话机 101（步骤 S546）。

便携式电话机 101 接收数据[[Kc, License]Kcard(1)]Ks1 后（步骤 S548），在存储器 120 中，解密处理部 1410 根据对话 Key Ks1 进行解密处理，抽出数据[Kc, License]Kcard(1)并存储于存储器 1412（步骤 S552）。

以下的处理与图 22 及图 23 所示实施方式 3 的处理相同，所以不再重复其说明。

通过如上结构，用户可以较简便地接受已加密的音乐数据等内容数据的分发。

而且，有如下效果，在数据总线上等所传送的数据的加密 Key 按各对话且按各设备变更，所以将进一步提高数据交换的安全性。

[实施方式 4 的变化例]

在实施方式 4 的数据分发系统中，形成如下结构：存储插件 120 通过便携式电话机 101 从内容数据销售机 3000 接受加密内容数据的分发。

但是，在图 27 所示的内容数据销售机 3000 的结构中，与实施方式 3 的变化例相同，如果取代插接件 2010，形成设置存储槽作为与存储插件 120 之间的接口的结构，则无需通过便携式电话机 101 就能够使存储插件 120 与内容数据销售机 3000 直接进行数据交换。

除了数据处理部 2100 的结构，如此实施方式 4 的变化例的内容数据销售机 3001 的结构与图 24 所示的实施方式 3 的变化例的结构相同。

即，实施方式 4 的变化例的内容数据销售机 3001 的结构与图 27 所示实施方式 4 的内容数据销售机 3000 的结构不同，其形成如下结构：取代外部插接件 2010，设置可插入存储插件的插件槽 2030，该插件槽 2030 通过接口部 2012 与数据总线 BS1 进行数据交换。

图 30 及图 31 为用以说明实施方式 4 的变化例的数据分发系统的分发模式的第 1 及第 2 流程图。

除了存储插件 120 与内容数据销售机 3001 不通过便携式电话机 101 而进行数据交换这一点，其与图 28 及图 29 所示实施方式 3 的分发模式的处理相同，所以对同一处理赋予同一符号而不再重复其说明。

通过如上结构及动作，用户可以更简便地接受已加密的音乐数据等的分发。

而且有这样的优点：存储插件可以独立接受并存放加密内容数据的分发，所以音乐再生单元的选择范围增大，将进一步提高用户的便利性。

[实施方式 5]

实施方式 5 的分发服务器 12、便携式电话机 105 及存储插件 140 如以下说明，其特征为：其与实施方式 2 的分发服务器 11、便携式电话机 101 及存储插件 120 的结构有以下不同之处。

即，在实施方式 5 的便携式电话机 105 中如具有将预先由分发系统的认证机构等管理部门在登录该便携式电话机 105 之际分配给该便携式电话机 105 的公开密码密钥 KPp 及证明数据 Crtf 以根据公开解密

密钥（公开认证密钥）KPmaster 加密后的形式加以记录保存的单元。

同样，在实施方式 5 的存储插件 140 中例如也具有预先由分发系统的认证机构等管理部门在登录该存储插件 140 之际分配给该存储插件的公开密码密钥 KPmedia 及证明数据 Crtf 以根据公开解密密钥（公开认证密钥）KPmaster 加密后的形式加以记录保存的单元。

在此，存储插件 140 及实施方式 5 的分发服务器 12 具有记录并保存该公开解密密钥（公开认证密钥）KPmaster 的单元。该公开解密密钥（公开认证密钥）KPmaster 为所有在系统中输出数据的设备在互换对话 Key 时用于证明其为可互相交换数据的设备和用于获取其向对方送交对话 Key 之际所用加密密钥的系统公用的解密密钥。

下面，进而对实施方式 5 的便携式电话机 105、存储插件 140 及分发服务器 12 的结构作较详细地说明。

图 32 为用以说明实施方式 5 的便携式电话机 105 的结构的概略框图。

其与图 12 所示实施方式 2 的便携式电话机 101 的结构的不同之处为其形成如下结构：取代 KPp 保存部 1524，其具备用以保存根据公开解密密钥（公开认证密钥）KPmaster 加密后的公开密码密钥 KPp 及证明数据 Crtf 的[KPp，Crtf]KPmaster 保存部 1525。

便携式电话机 105 的其他各处与图 12 所示实施方式 2 的便携式电话机 101 的结构相同，所以对同一部分赋予同一符号而不再重复其说明。

图 33 为表示实施方式 5 的存储插件 140 所对应的分发服务器 12 的结构的概略框图。其与图 11 所示实施方式 2 的分发服务器 11 的结构的不同之处为其形成如下结构：数据处理部 310 还具备保存公开解密密钥 KPmaster 的 KPmaster 保存部 324 和用以根据从 KPmaster 保存部 324 所输出的公开解密密钥 KPmaster 将通过通信装置 350 从通信网提供给数据总线 BS1 的数据解密的解密处理部 326。加密处理部 316 根据由解密处理部 326 的解密处理所抽出的公开加密密钥 KPmedia 将 Ks 发生部 314 所产生的对话 Key Ks 加密，另外，分发控制部 312 根据由解密处理部 326 的解密处理所抽出的证明数据 Crtf 对请求分发的存储插件及便携式电话机是否正规进行认证。

分发服务器 12 的其他各处与图 12 所示实施方式 2 的分发服务器

11 的结构相同，所以对同一部分赋予同一符号而不再重复其说明。

图 34 为用以说明本发明的实施方式 5 的存储插件 140 的结构的概略框图，也是与实施方式 2 的图 13 的对比图。

实施方式 5 的存储插件 140 的结构与实施方式 2 的存储插件 120 的结构的不同之处为其形成如下结构：首先，存储插件 140 具备将公开密码密钥 KPmedia 及证明数据 Crtf 以根据公开解密密钥（公开认证密钥）KPmaster 加密后的形式进行记录保存的 [KPmedia，Crtf]KPmaster 保存部 1442。另一方面，省略切换开关 1436、[KPmedia，Crtf]KPmaster 保存部 1442 的输出直接提供给数据总线 BS3。

其次，存储插件 140 具备用以记录保存公开解密密钥 KPmaster 的 KPmaster 保存部 1450 和用以根据从 KPmaster 保存部 1450 所输出的公开解密密钥 KPmaster 将数据总线 BS3 上的数据解密的解密处理部 1452。

由解密处理部 1452 的解密处理所抽出的公开加密密钥 KPmedia 及证明数据 Crtf 中的公开加密密钥 KPmedia 被提供给加密处理部 1430，证明数据 Crtf 通过数据总线 BS5 被提供给控制器 1420。

存储插件 140 的其他结构与图 13 所示存储插件 120 的结构相同，所以对同一部分赋予同一符号而不再重复说明。

[分发模式]

图 35 及图 36 为用以说明采用了以图 34 说明的存储插件 140 的分发模式的第 1 及第 2 流程图。

在图 35 及图 36 中也对用户 1 用装载了存储插件 140 的便携式电话机 105 从分发服务器 12 接受内容数据的分发时的动作进行说明。

首先，从用户 1 的便携式电话机 105 由用户通过对接触密钥 1108 的按密钥操作进行分发请求（步骤 S100）。

另外，为了区别于其他存储插件的公开加密密钥 KPmedia，将存储插件 140 中所保存的公开加密密钥 Kpmedia 设为公开加密密钥 KPmedia(1)。再有，将存储插件 140、便携式电话机 105 的证明数据分别设为 Crtf(1)、Crtf(p)。

在存储插件 140 中，对应该分发请求，从 [KPmedia，Crtf]KPmaster 保存部 1442 向便携式电话机 105 输出将公开加密密钥 KPmedia（1）

及证明数据 Crtf(1)加密后的数据[KPmedia(1), Crtf(1)]KPmaster（步骤 S102 ）.

在便携式电话机 105 中，与来自存储插件 140 的数据[KPmedia(1), Crtf(1)]KPmaster 一起，将来自[KPp, Crtf]KPmaster 保存部 1525 的数据[KPp, Crtf(p)]KPmaster、分发请求发送给分发服务器 12（步骤 S103）.

在分发服务器 12 中，接收从存储插件 140 所传递的分发请求及数据[KPp, Crtf(p)]KPmaster、[KPmedia(1), Crtf(1)]KPmaster 后（步骤 S104 ），解密处理部 326 根据公开解密密钥 KPmaster 进行解密处理，抽出证明数据 Crtf(1)、Crtf(p)、公开加密密钥 KPp、公开加密密钥 KPmedia(1)（步骤 S105）.

分发控制部 312 根据解密后的证明数据 Crtf(1)及 Crtf(p)向分发服务器 12 进行查询，当存储插件和便携式电话机的证明数据 Crtf(1)及 Crtf(p)皆为正规的证明数据时移至下一处理（步骤 S S106 ），当之一为非正规的证明数据时结束处理（步骤 S154）.

查询结果确认为正规的证明数据后，则分发服务器 12 中的对话 Key 发生部 314 生成对话 Key Ks. 进而，分发服务器 12 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1)将该对话 Key Ks 加密并生成加密对话 Key[Ks]Kmedia(1)（步骤 S108）.

接下来，分发服务器 12 将加密对话 Key[Ks]Kmedia(1)提供给数据总线 BS1. 通信装置 350 通过通信网将来自加密处理部 316 的加密对话 Key[Ks]Kmedia(1)发送给便携式电话机 105 的存储插件 140（步骤 S110）.

便携式电话机 105 接收加密对话 Key[Ks]Kmedia(1)后（步骤 S112），在存储插件 140 中，解密处理部 1404 用秘密解密密钥 Kmedia(1)对通过存储器接口 1200 提供给数据总线 BS3 的接收数据进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S114）.

进而，在存储插件 140 中，由 Ks1 发生部 1432 生成对话 Key Ks1（步骤 S115）.

接下来，在分发模式中，切换开关 1409 的接点 Pa 或 Pb 依次选择闭合状态，所以加密处理部 1406 根据对话 Key Ks 将通过接点 Pa 从对话 Key 发生部 1432 所提供的对话 Key Ks1 和通过接点 Pb 从 KPcard(1)

保存部1405所提供的公开加密密钥KPcard(1)(对于存储插件140的公开加密密钥)加密(步骤S116),生成数据[KPcard(1)、Ks1]Ks(步骤S118)。

便携式电话机105将由加密处理部1406所加密的数据[KPcard(1)、Ks1]Ks发送给分发服务器12(步骤S120)。

在分发服务器12中,由通信装置350接收数据[KPcard(1)、Ks1]Ks(步骤S122),解密处理部318根据对话Key Ks对提供给数据总线BS1的数据[KPcard(1)、Ks1]Ks进行解密处理,将公开加密密钥KPcard(1)及对话Key Ks1解密抽出(步骤S124)。

接下来,分发控制部312以分发信息数据库304等所保存的数据为基础生成含有许可ID数据等的许可信息数据License(步骤S126)。

进而,分发服务器12从分发信息数据库304获得加密内容数据[Dc]Kc并通过通信装置350发送给存储插件140(步骤S128)。

便携式电话机105接收加密内容数据[Dc]Kc后(步骤S130),在存储插件140中,将接收到的加密内容数据[Dc]Kc直接存放于存储器1412(步骤S132)。

另一方面,分发服务器12从分发信息数据库304获得许可Key Kc(步骤S134),加密处理部320根据由解密处理部318所提供的公开加密密钥KPcard(1)对来自分发控制部312的许可Key Kc和许可信息数据License进行加密处理(步骤S136)。

加密处理部322收到由加密处理部320所加密的数据[Kc、License]Kcard(1),进而将根据来自存储插件140的对话Key Ks1加密后的数据提供给数据总线BS1。通信装置350将由加密处理部322所加密的数据[[Kc, License]Kcard(1)]Ks1发送给存储插件140。

便携式电话机105接收数据[[Kc, License]Kcard(1)]Ks1后(步骤S142),在存储插件140中,解密处理部1410根据通过接点Pf从Ks1发生部1432所提供的对话Key Ks1进行解密处理,抽出数据[Kc, License]Kcard(1)并存放于存储器1412(步骤S146)。

进而,在存储插件140中,在控制器1420的控制下,解密处理部1416将存储器1412所存放的数据[Kc, License]Kcard(1)解密,并将已解密的许可信息数据License存放于寄存器1500(步骤S148)。

通过如上动作,存储插件140本身可以向加密内容数据的发送侧

（分发服务器 12）发送公开加密密钥 KPmedia(1)及对话 Key Ks1，在此之上接受分发，存储插件 140 成为可再生音乐的状态。

进而，存储插件 140 向分发服务器 12 发出分发受理通知，分发服务器 12 接收分发受理后（步骤 S150），用户 1 的收费数据被存放于收费数据库 302（步骤 S152），处理结束（步骤 S154）。

在如上的分发模式中，在对存储插件及便携式电话机加以认证之后进行内容数据的分发，所以系统的安全性及版权保护将得到进一步加强。

[再生模式]

图 37 及图 38 为说明用以在便携式电话机 105 内从存储插件 140 所保存的加密内容数据将音乐信号解密并作为音乐输出到外部的再生处理的第 1 及第 2 流程图。

参照图 37 及图 38，根据来自便携式电话机 105 的接触密钥 1108 等的用户 1 的指示，向便携式电话机 105 输出再生请求（步骤 S200）。

与此对应，从便携式电话机 105 向存储插件 140 发送数据[KPp，Ctrf(p)]KPmaster（步骤 S241）。

在存储插件 140 中，接收数据[KPp，Ctrf(p)]KPmaster 后，则由解密处理部 1452 进行解密处理并抽出公开加密密钥 KPp 及数据 Crtf（步骤 S243）。

根据所抽出的证明数据 Crtf，控制器 1420 判断便携式电话机 105 是否为正规设备（步骤 S245），当判断为正规设备时，处理移至下一步骤 S246，当判断为非正规设备时，结束处理（步骤 S280）。

当判断为正规设备时，在存储插件 140 中生成对话 Key Ks1（步骤 S246）。存储插件 140 进而根据所抽出的公开加密密钥 KPp 将对话 Key Ks1 加密（步骤 S248），并将所生成的加密对话 Key[Ks1]Kp 发送给便携式电话机 105（步骤 S250）。

在便携式电话机 105 中，接收来自存储插件 140 的加密对话 Key[Ks1]Kp 后，则解密处理部 1522 根据秘密解密密钥 Kp 进行解密并抽出在存储插件 140 中生成的对话 Key Ks1（步骤 S252）。接下来，Ks 发生部 1502 生成对话 Key Ks（步骤 S253），便携式电话机 105 的加密处理部 1504 根据对话 Key Ks1 将便携式电话机 105 中生成的对话 Key Ks 加密并生成加密对话 Key[Ks]Ks1（步骤 S254），并将该加密

对话 Key[Ks]Ks1 发送给存储插件 140（步骤 S256）。

存储插件 140 通过数据总线 BS2 收到由便携式电话机 105 所生成且已加密的对话 Key Ks，根据对话 Key Ks1 解密并抽出便携式电话机 105 中生成的对话 Key Ks（步骤 S258）。

接下来，在存储插件 140 中，控制器 1420 根据寄存器 1500 所保存的许可信息数据 License 判断是否可解密（步骤 S259），当判断为可解密时，移至下一处理，当判断为不可解密时结束处理（步骤 S280）。

接下来，存储插件 140 从存储器 1412 读出已加密的数据[Kc, License]Kcard(1)，解密处理部 1416 进行解密处理（步骤 S260）。

当根据秘密解密密钥 Kcard(1)可将从存储器 1412 读出的数据解密时（步骤 S262），抽出许可 Key Kc（步骤 S264）。另一方面，在不能解密时，处理结束（步骤 S280）。

当可将从存储器 1412 读出的数据解密时，进而在寄存器 1500 内的许可信息数据 License 中的有关再生次数的数据被变更（步骤 S266）。

接下来，在存储插件 140 中，加密处理部 1406 根据抽出的对话 Key Ks 将许可 Key Kc 加密（步骤 S268），并将加密后的许可 Key[Kc]Ks 提供给数据总线 BS2（步骤 S270）。

便携式电话机 105 的解密处理部 1506 根据对话 Key Ks 进行解密处理，据此获得许可 Key Kc（步骤 S272）。

接下来，存储插件 140 从存储器 1412 读出加密内容数据[Dc]Kc 并提供给数据总线 BS2（步骤 S274）。

便携式电话机 105 的音乐再生部 1508 根据所抽出的许可 Key Kc 对加密内容数据[Dc]Kc 进行解密处理生成普通文的内容数据（步骤 S276），并从内容数据再生音乐信号提供给混合部 1510（步骤 S276）。数模转换部 1512 收到来自于混合部 1510 的数据并转换，将所再生的音乐输出至外部，处理结束（步骤 S232）。

通过形成如上结构，存储插件本身及便携式电话机本身能够分别生成对话 Key Ks1 或 Ks，据此进行加密内容数据的交换，在此之上进行再生动作。

进而，存储插件 140 对便携式电话机 105 进行认证，在此之上进行再生动作，所以将提高系统的安全性及版权保护。

[移动或复制模式]

图 39 及图 40 为有以说明在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 1 及第 2 流程图.

首先，设具有与便携式电话机 105 相同结构的便携式电话机 106 为发送侧，便携式电话机 105 为接收侧. 另外，便携式电话机 106 也装载具有与存储插件 140 相同结构的存储插件 142.

便携式电话机 106 首先向便携式电话机 105 输出移动请求或复制请求（步骤 S300）.

便携式电话机 105 接收该请求后（步骤 S301），存储插件 142 与此对应，读出存储器 1412 内的加密内容数据[Dc]Kc 并向存储插件 140 输出（步骤 S302），存储插件 140 将加密内容数据[Dc]Kc 存放于存储器 1412（步骤 S304）.

接下来，在便携式电话机 106 及 105 中，判断在步骤 S300 所提供的请求是“移动请求”还是“复制请求”（步骤 S306、步骤 S306 ），当为“移动请求”时，存储插件 140 对应该移动请求从[KPmedia, Crtf]KPmaster 保存部 1442 向便携式电话机 105 输出将公开加密密钥 KPmedia(1) 及证明数据 Crtf(1) 加密后的数据 [KPmedia(1), Crtf(1)]KPmaster（步骤 S307）.

便携式电话机 105 将来自存储插件 140 的数据[KPmedia(1), Crtf(1)]KPmaster 发送给便携式电话机 106（步骤 S308）.

便携式电话机 106 接收从存储插件 140 所传递的数据 [KPmedia(1), Crtf(1)]KPmaster 后（步骤 S309），存储插件 142 内的解密处理部 1452 进行解密处理，抽出证明数据 Crtf(1)、公开加密密钥 KPmedia(1)（步骤 S310）.

控制器 1420 根据已解密的证明数据 Crtf(1) 进行认证，当为来自正规存储插件的访问时移至下一处理（步骤 S311），当为非正规存储插件时，便携式电话机 106 发送不可移动的通知，同时存储插件 142 结束处理（步骤 S374）. 便携式电话机 105 接收不可移动通知后（步骤 S313），存储插件 140 也结束处理（步骤 S374）.

另一方面，在步骤 S311 的查询结果确认为正规存储插件后，则存储插件 142 的 Ks2 发生电路 1432 生成对话 Key Ks2（步骤 S314），加密处理部 1430 用公开加密密钥 KPmedia(1) 将对话 Key Ks2 加密(步

骤 S315）.

便携式电话机106将加密对话Key[Ks2]KPmedia(1)发送给便携式电话机 105（步骤 S316）. 便携式电话机 105 接收加密对话 Key[Ks2]KPmedia(1)后（步骤S318）传送给存储插件140，存储插件 140 的解密处理部 1404 进行解密，受理对话 Key Ks2（步骤 S320）. 进而，在存储插件 140 中生成对话 Key Ks1（步骤 S321）.

在存储插件 140 中，根据对话 Key Ks2 将存储插件 140 的公开加密密钥 KPcard(1)及对话 Key Ks1 加密（步骤 S322），从便携式电话机 105 向便携式电话机 106 发送所加密的数据[KPcard(1)、Ks1]Ks2（步骤 S324）. 便携式电话机 106 接收数据[KPcard(1)、Ks1]Ks2（步骤 S326），并传递给存储插件 142.

在存储插件 142 中，解密处理部 1410 根据对话 Key Ks2 将从存储插件 140 所发送的加密数据[KPcard(1)、Ks1]Ks2 解密，并将存储插件 140 的公开加密密钥 KPcard(1)、对话 Key Ks1 解密抽出.（步骤 S330）.

接下来，在存储插件 142 中，从存储器 1412 读出根据存储插件 142 的公开加密密钥 KPcard(2)加密后的许可 Key Kc、许可信息数据 License 所对应的[Kc、License]Kcard(2)（步骤 S332）.

接下来，存储插件 142 的解密处理部 1416 根据秘密解密密钥 Kcard(2)对许可 Key Kc、许可信息数据 License 进行解密处理（步骤 S334）.

存储插件 142 的控制器 1420 将经过如此解密的许可信息数据 License 的值与寄存器 1500 内的数据值进行置换（步骤 S336）.

进而，存储插件 142 的加密处理部 1414 根据在解密处理部 1410 中所抽出的存储插件 140 的公开加密密钥 KPcard(1)将许可 Key Kc、许可信息数据 License 加密（步骤 S338）.

由存储插件 142 的加密处理部 1414 所加密的数据通过切换开关 1409（接点 Pd 闭合）再提供给加密处理部 1406，存储插件 142 的加密处理部 1406 根据对话 Key Ks1 将数据[Kc，License]Kcard(1)加密并生成数据[[Kc，License]Kcard(1)]Ks1（步骤 S340）.

接下来，存储插件 142 向便携式电话机 106 输出数据[[Kc，License]Kcard(1)]Ks1(步骤 S342)，便携式电话机 106 将数据[[Kc，

License]Kcard(1)]Ks1 发送给便携式电话机 105（步骤 S344）。

便携式电话机105接收到的数据[[Kc,License]Kcard(1)]Ks1(步骤 S346)被传送给存储插件 140，存储插件 140 的解密处理部 1410 将已加密的数据[[Kc，License]Kcard(1)]Ks1 解密，受理数据[Kc，License]Kcard(1)（步骤 S348）。

在存储插件 140 中，将由解密处理部 1410 根据对话 Key Ks1 进行解密处理后的数据[Kc，License]Kcard(1)存放于存储器 1412（步骤 S350）。进而，在存储插件 140 中，解密处理部 1416 根据秘密解密密钥 Kcard(1)将数据[Kc，License]Kcard(1)解密，并将所解密的许可信息数据 License 存放于寄存器 1500（步骤 S352）。

以后的移动模式的处理以及复制模式中的存储插件 140 及 142 的处理与以图 18 及图 19 说明的实施方式 2 的存储插件 120、122 等的处理相同，所以不再重复其说明。

通过形成如此结构，移动源及移动目标的存储插件本身能够分别生成对话 Key，在此之上进行移动动作及复制动作。

因此，有这样的效果：在数据总线上等所传送的数据的加密 Key 按各对话且按各设备变更，所以将进一步提高数据交换的安全性。

而且，通过使用如上结构，有这样的效果：例如不通过具有如上所述的对话 Key 发生电路 1502 的携带电话终端而由能够连接存储插件与存储插件的接口设备也能够进行从存储插件 142 向存储插件 140 的数据移动，将进一步提高用户的便利性。

在此，在移动模式时，关于限制再生信息内的再生次数的许可信息数据，通过将存储器 1412 所记录的许可信息数据变更为记录有在寄存器 1500 中每次再生都被修正的再生次数的许可信息数据而对许可信息数据进行更新。这样，即使在存储插件之间移动内容数据，也可使再生次数有限制的内容数据的再生次数不会超过分发时所决定的再生次数的限制。

而且，存储插件 142 对存储插件 140 进行认证，在此之上进行移动动作，所以将提高系统的安全性及版权保护。

[实施方式 6]

图 41 为表示本发明的实施方式 6 的内容数据销售机 3010 的结构的概略框图，也是与实施方式 4 的图 27 的对比图。

不过，在以下说明中，形成如下结构：设置存储槽 2030 作为与实施方式 5 中说明的存储插件 140 之间的接口，与实施方式 4 的变化例相同，存储插件 140 与内容数据销售机 3010 无需通过便携式电话机 105 而直接进行数据的交换。

当然也可形成如下结构：凭借插接件 2010，存储插件 140 与内容数据销售机 3010 通过便携式电话机 105 进行数据的交换。

因此，内容数据销售机 3010 的结构与实施方式 4 的内容数据销售机 3000 的结构的不同之处为：设置存储槽 2030 以取代插接件 2010；数据处理部 2100 形成再具备保存公开解密密钥 KPmaster 的 KPmaster 保存部 324、用以根据从 KPmaster 保存部 324 所输出的公开解密密钥 KPmaster 将通过通信装置 350 从通信网提供给数据总线 BS1 的数据解密的解密处理部 326 的结构。加密处理部 316 根据由解密处理部 326 的解密处理所抽出的公开加密密钥 KPmedia 将 Ks 发生部 314 所产生的对话 Key Ks 加密，另外，分发控制部 312 根据由解密处理部 326 的解密处理所抽出的证明数据 Crtf，对请求分发的存储插件是否为正规的存储插件进行认证。

内容数据销售机 3010 的其他各处与图 27 所示实施方式 4 的内容数据销售机 3000 的结构相同，所以对同一部分赋予同一符号而不再重复其说明。

[分发模式]

图 42 及图 43 为用以说明采用了以图 41 说明的内容数据销售机 3010 的分发系统的分发动作的第 1 及第 2 流程图。

在图 42 及图 43 中，对用户 1 通过采用了存储插件 140 从内容数据销售机 3010 接受内容数据（音乐数据）的分发时的动作进行说明。

首先，用户通过对内容数据销售机 3010 的密钥盘 2004 的按密钥操作等发出分发请求指示（步骤 S500）。

从内容数据销售机 3010 向存储插件 140 输出用以认证的数据 [KPmedia，Crtf]KPmaster 的发送要求（步骤 S502 ）。

在存储插件 140 中，对应该发送要求，从 [KPmedia，Crtf]KPmaster 保存部 1442 向内容数据销售机 3010 输出将公开加密密钥 KPmedia (1) 及证明数据 Crtf (1) 加密后的数据 [KPmeida (1)，Crtf (1)]KPmaster（步骤 S507）。

内容数据销售机 3010 接收从存储插件 140 所传递的数据 [KPmedia(1), Crtf(1)]KPmaster 后，解密处理部 326 根据公开解密密钥 KPmaster 进行解密处理，抽出证明数据 Crtf(1)、公开加密密钥 KPp、公开加密密钥 KPmedia(1)（步骤 S509）。

根据所解密的证明数据 Crtf(1)，分发控制部 312 对是否为来自正规存储插件的访问进行判断。当为正规的存储插件时移至下一处理（步骤 S511），当为非正规存储插件时，将异常结束记录存放于管理服务器 2200 中的管理数据库（步骤 S561），结束处理（步骤 S562）。

内容数据销售机 3010 在步骤 S511 的查询结果确认为正规存储插件后，通过显示器 2002 引导用户投入费用，并收取费用（步骤 S512）。

接下来，内容数据销售机 3010 的对话 Key 发生部 314 生成对话 Key Ks。进而，内容数据销售机 3010 内的加密处理部 316 根据接收到的公开加密密钥 KPmedia(1) 将该对话 Key Ks 加密并生成加密对话 Key[Ks]Kmedia(1)（步骤 S514）。

接下来，内容数据销售机 3010 将加密对话 Key[Ks]Kmedia(1) 提供给数据总线 BS1，并从插件槽 2030 输出（步骤 S516）。

在存储插件 140 中，解密处理部 1404 根据秘密解密密钥 Kmedia(1) 对通过存储器接口 1200 提供给数据总线 BS3 的加密对话 Key[Ks]Kmedia(1) 进行解密处理，据此将对话 Key Ks 解密并抽出（步骤 S520）。进而，在存储插件 140 中生成对话 Key Ks1（步骤 S521）。

接下来，在分发模式中，切换开关 1408 选择处于闭合状态的接点 Pa，所以加密处理部 1406 根据对话 Key Ks 将通过接点 Pa 从 KPcard(1) 保存部 1405 所提供的公开加密密钥 KPcard(1) 加密（步骤 S522），生成数据 [KPcard(1)]Ks（步骤 S524）。

在内容数据销售机 3010 中，通过插件槽 2030 接收数据 [KPcard(1)]Ks（步骤 S528），解密处理部 318 根据对话 Key Ks 对提供给数据总线 BS1 的数据 [KPcard(1)]Ks 进行解密处理，将公开加密密钥 KPcard(1) 解密抽出（步骤 S530）。

接下来，分发控制部 312 以分发信息数据库 304 等所保存的数据为基础生成含有许可 ID 数据等的许可信息数据 License（步骤 S532）。

进而，内容数据销售机 3010 从分发信息数据库 304 获得加密内容数据 [Dc]Kc，通过插件槽 2030 发送给存储插件 140（步骤 S534）。

在存储插件 140 中，将接收到的加密内容数据[Dc]Kc 直接存放于存储器 1412（步骤 S538）。

另一方面，内容数据销售机 3010 从分发信息数据库 304 获得许可 Key Kc（步骤 S540），加密处理部 320 根据由解密处理部 318 所提供的公开加密密钥 KPcard(1)对来自分发控制部 312 的许可 Key Kc 和许可信息数据 License 进行加密处理（步骤 S542）。

加密处理部 322 收到由加密处理部 320 加密后的数据[Kc、License]Kcard(1)，并将根据对话 Key Ks 再行加密的数据提供给数据总线 BS1，由加密处理部 322 加密后的数据[[Kc，License]Kcard(1)]Ks1 被发送给存储插件 140（步骤 S546）。

在存储插件 140 中，解密处理部 1410 根据对话 Key Ks1 进行解密处理，抽出数据[Kc，License]Kcard(1)并存放于存储器 1412（步骤 S552）。

进而，在存储插件 140 中，在控制器 1420 的控制下，解密处理部 1416 将存储器 1412 中所存放的数据[Kc，License]Kcard(1)解密，并将所解密的许可信息数据 License 存放于寄存器 1500（步骤 S554）。

通过如上动作，存储插件 140 成为可从内容数据再生音乐的状态。

进而，从存储插件 140 向内容数据销售机 3010 发出分发受理通知（步骤 S558），内容数据销售机 3010 接收分发受理后，将销售记录发送给管理服务器 2200 中的管理数据库（步骤 S560），处理结束（步骤 S562）。

通过如上结构，用户可以更简便地接受已加密的音乐数据等内容数据的分发。而且，是在存储插件经过认证之后进行内容数据的分发的，所以将进一步加强系统的安全性及版权保护。

[实施方式 7]

图 44 为用以说明实施方式 7 的便携式电话机 107 的结构的概略框图。

其与图 32 所示实施方式 5 的便携式电话机 105 的结构的不同之处为其形成具备如下各部的结构：保存便携式电话机这一再生装置所通用的解密密钥 Kcom 的 Kcom 保存部 1530；接受解密处理部 1506 的输出，就解密密钥 Kcom 进行解密，并将许可 Key Kc 提供给音乐再生部 1508 的解密处理部 1532。

便携式电话机107的其他各处与图32所示实施方式5的使携式电话机105的结构相同，所以对同一部分赋予同一符号而不再重复其说明。存储插件140的结构也相同。

即，实施方式7除了在实施方式5中向音乐再生部1508最终提供许可Key Kc之前，在实施方式7中是将构成系统的各设备之间所交换的许可Key Kc以再行加密后的[Kc]Kcom的形式进行互换之外，其与实施方式5的结构相同。

另外，在以下的说明中是以解密密钥Kcom为公用密钥作以说明，但本发明并不局限于此种情况，例如也可以形成以公开密钥KPcom进行加密、以与公开加密密钥KPcom非对称的秘密解密密钥Kcom进行解密的结构。

图45为表示对应于实施方式7的便携式电话机107的分发服务器13的结构的概略框图。其与图33所示实施方式5的分发服务器12的结构的不同之处为数据处理部310形成再具备如下各部的结构：保存解密密钥Kcom的Kcom保存部330；根据解密密钥Kcom对通过分发控制部312从分发信息数据库304所提供的许可Key Kc进行加密处理，并作为加密许可Key[Kc]Kcom提供给加密处理部320的加密处理部332。

分发服务器13的其他各处与图33所示实施方式5的分发服务器12的结构的结构相同，所以对同一部分赋予同一符号而不再重复其说明。

[分发模式]

图46及图47为用以说明采用了以图44及45说明的分发服务器13和便携式电话机107的分发模式的第1及第2流程图。

在图46及图47中也对用户1通过采用了存储插件140从分发服务器13接受内容数据（音乐数据）的分发时的动作进行说明。

不过，除了在步骤S134中分发服务器13从分发信息数据库304获得许可Key Kc后，加密处理部332将Key Kc加密（步骤S135），以后作为加密许可Key[Kc]Kcom进行交换之外，图46及图47的处理与以图35及图36说明的实施方式5的分发模式相同，所以不再重复其说明。

如上分发模式与实施方式5相比将进一步加强系统的安全性。

[再生动作]

图 48 及图 49 为说明用以在便携式电话机 107 内从存储插件 140 所保存的加密内容数据再生音乐信号并作为音乐输出至外部的再生处理的第 1 及第 2 流程图.

不过，除了在步骤 S264 从存储插件 140 的存储器 1412 所读出的 Key 为加密许可 Key[Kc]Kcom，以后作为加密许可 Key[Kc]Kcom 发送给便携式电话机 107，在便携式电话机 107 中在步骤 S273 由解密处理部 1532 将 Key[Kc]Kcom 解密并将许可 Key Kc 提供给音乐再生部 1508 之外，图 48 及图 49 所示再生处理与图 37 及图 38 所示实施方式 5 的再生处理相同，所以不再重复其说明.

通过形成如此结构，将进一步提高再生模式的系统的安全性及版权的保护.

[移动或复制模式]

图 50 及图 51 为用以说明在实施方式 7 中在两个存储插件之间进行内容数据及 Key 数据等的移动或复制处理的第 1 及第 2 流程图.

不过，除了许可 Key Kc 作为加密许可 Key[Kc]Kcom 进行交换之外，图 50 及图 51 的处理与以图 39 及图 40 说明的实施方式 5 的移动或复制模式的动作相同，所以不再重复其说明.

通过形成如此结构，将进一步提高移动或复制模式的系统的安全性及版权的保护.

[实施方式 8]

图 52 为表示本发明的实施方式 8 的内容数据销售机 3020 的结构的概略框图，也是与实施方式 6 的图 41 的对比图.

内容数据销售机 3020 的结构与实施方式 6 的内容数据销售机 3010 的结构的不同之处为数据处理部 2100 形成再具备如下各部的结构：保存解密密钥 Kcom 的 Kcom 保存部 330；根据解密密钥 Kcom 对通过分发控制部 312 从分发信息数据库 304 所提供的许可 Key Kc 进行加密处理，并作为加密许可 Key[Kc]Kcom 提供给加密处理部 320 的加密处理部 332.

内容数据销售机 3020 的其他各处与图 41 所示实施方式 6 的内容数据销售机 3010 的结构的结构相同，所以对同一部分赋予同一符号而不再重复其说明.

当然，实施方式 8 也可以形成凭借插接件 2010，存储插件 140 与内容数据销售机 3020 通过便携式电话机 107 进行数据交换的结构。

[分发模式]

图 53 及图 54 为用以说明采用了以图 52 说明的内容数据销售机 3020 的数据分发系统的分发模式的第 1 及第 2 流程图。

在图 53 及图 54 中对用户 1 通过采用了存储插件 140 从内容数据销售机 3020 接受内容数据（音乐数据）的分发时的动作进行说明。

不过，除了在步骤 S540 内容数据销售机 3020 从分发信息数据库 304 获得许可 Key Kc 后，加密处理部 332 将许可 Key Kc 加密（步骤 S541），以后作为加密许可 Key[Kc]Kcom 进行交换之外，图 53 及图 54 的处理与以图 42 及图 43 说明的实施方式 5 的分发动作相同，所以不再重复其说明。

如上分发模式与实施方式 6 相比将进一步加强系统的安全性。

在此按先分发加密内容数据并存放于存储插件 110、120、140 内的存储器 1412 再接受许可 Key Kc、许可信息数据 License 的分发作了说明，反之，先分发许可 Key Kc、许可信息数据 License 并存放于存储插件 110、120、140 内的寄存器 1500 再接受加密内容数据的分发也没关系。

再有，在移动模式中也与分发模式相同，加密内容数据、许可 Key Kc、许可信息数据 License 中哪一方移动为先都没关系。

另外，在以上说明的各实施方式中，也可以将作为分发数据随附于内容数据的非加密数据例如上述音乐数据的曲名、表演者（歌手、演奏者等）、作曲家、作词家等有关该音乐数据（内容数据）的作品信息和用以对分发服务器 10、11、内容数据销售机 3000、3001 进行访问的信息等作为附加数据 Di 与加密内容数据合并分发。该附加数据 Di 与加密内容数据同样存放于存储器 1412 以能够在分发、移动、复制中与内容数据一同处理，在再生时分离并与内容数据分别访问。

[实施方式 9]

图 55 为说明以上说明过的存储插件 110、120、140 等的端子 1202 部分的结构的概略框图。

以下就存储插件 140 的端子 1202 部分的结构作以说明。

数据和命令通过端子 1202 被串行提供给存储插件 140。与此相

反，令数据和命令被并行传送给存储插件 140 中的数据总线 BS3。

图 55 为表示在向这样的存储插件 140 输入数据时进行串行、并行转换和在输出数据时进行并行、串行转换的结构的概略框图。

用于对数据输入输出的时机进行指定的信号即信号 CS 被提供给端子 1202 中的数据引脚 1460。例如通过提供给数据输入引脚 1462 的数据在信号 CS 激活（“L”电位）之后的规定期间后变为“L”电位检测出数据输入的时机。同样，通过输出至数据输出引脚 1464 的数据在信号 CS 激活（“L”电位）之后的规定期间后变为“L”电位检测出数据输出的时机。接口控制器 1490 管理从存储插件 140 的外部向数据总线 BS3 的数据输入以及从数据总线 BS3 向存储插件 140 外部的数据输出。

在数据输入时，提供给数据输入引脚 1462 的数据通过缓冲器 1468 输入至纵行连接的 D—触发器 1470.0～1470.7。即，在 8 比特的数据被输入的时点，D—触发器 1470.0～1470.7 的所有数据被更新，在该时点，在接口控制器 1490 的控制下，数据从数据缓冲器 1427.0～1427.7 并行输出给数据总线 BS3。

在数据输出时，来自数据总线 BS3 的数据通过多路转换缓冲器 1476.1～1476.7 并行提供且存放于 D—触发器 1474.0～1474.7。之后在接口控制器 1490 的控制下，多路转换缓冲器 1476.1～1476.7 的连接切换，D—触发器 1474.0～1474.7 被纵行连接。在此状态，分别存放于 D—触发器 1474.0～1474.7 的数据通过由接口控制器 1490 控制的输出缓冲器 1470 从数据输出引脚 1464 依次串行输出。

[实施方式 9 的变化例]

图 56 为用以说明可将数据输入引脚的支数从 1 支变为 2 支或 4 支以提高数据输入速度的存储插件 140 的端子 1202 部分的结构的变化例的概略框图。

其与图 55 所示结构的不同之处为：首先，其设置有 4 支数据输入引脚 1462.0～1462.3 及与之对应的输入缓冲器 1468.0～1468.3；其形成再具备用以将提供给这些数据输入引脚 1462.0～1462.3 的命令从输入缓冲器 1468.0～1468.3 传送给接口控制器 1490 的多路转换缓冲器 1467 和用以将提供给数据输入引脚 1462.0～1462.3 的数据或命令从输入缓冲器 1468.0～1468.3 有选择地提供给 D—触发器 1470.0～1470.7 的多路转换缓冲器 1469.1～1469.7 的结构。

接着对动作加以简单说明。

载入电源后，例如存储插件140成为仅从1支数据输入引脚1462.0受理数据输入的状态。

下面，通过接口控制器1490根据从外部经由数据输入引脚1462.0～1462.3及多路转换缓冲器1467提供给接口控制器的命令对多路转换缓冲器1469.1～1469.7的控制，将来自4支数据输入引脚1462.0～1462.3的数据的动作模式变更为并行输入模式。

首先，在第1时机，提供给4支数据输入引脚1462.0～1462.3的数据经由多路转换器1469.1～1469.3提供给D—触发器1470.0～1470.3。

在接着的第2时机，多路转换器1469.1～1469.7切换连接，D—触发器1470.0～1470.3的输出分别提供给并存放于D—触发器1470.0～1470.7.进而在第3时机，提供给4支数据输入引脚1462.0～1462.3的数据经由多路转换器1469.1～1469.3提供给D—触发器1470.0～1470.3。

这样，8比特的数据向D—触发器1470.0～1470.7的存放结束。以后与图55的情况相同，8比特的数据并行提供给数据总线BS3。

数据输出时的动作与图55的情况相同。

通过如上结构，可以缩短在数据分发时尤其在从内容数据销售机2000等购买内容数据时对存储插件140的数据分发时间。

另外，在以上说明的各实施方式中，在分别装载于两部便携式电话机的两个存储插件之间，例如通过对PHS无线电收发信模式的利用，在说明了进行内容数据的移动处理的实施方式中可以不受此种结构限制，例如在一部便携式电话机能够同时装载多个存储插件时，可以形成通过在该便携式电话机上同时装载两个存储插件来进行内容数据的移动的结构。如此内容数据移动的情况，可以在以上说明的各实施方式中省略在两部便携式电话机间的收发信的往来。

另外，以上说明的各实施方式是按照将许可Key Kc以已加密的形式存放于存储器1412加以说明的，但也可以将许可Key Kc以已解密的普通文形式存放于寄存器1500。这是因为即使形成这种结构，寄存器1500设置在TRM区域内，也不能从外部读出许可Key Kc。

再有，以上说明的各实施方式是以可拆装于便携式电话机100等

的存储插件来存放加密内容数据[Dc]Kc 和许可 Key Kc 的，但也可以形成在便携式电话机内置入具有与此种存储插件等同功能的电路的结构．这种情况下，存储插件的种类和按各存储插件所规定的密钥可以视作被如此置入的电路的种类和按该各电路所规定者．

虽然，详细地说明并阐示了本发明，但这仅以例示为目的，而不成为限定，发明的思想和范围仅由附带的权利要求书所限定，这显然可以理解吧．

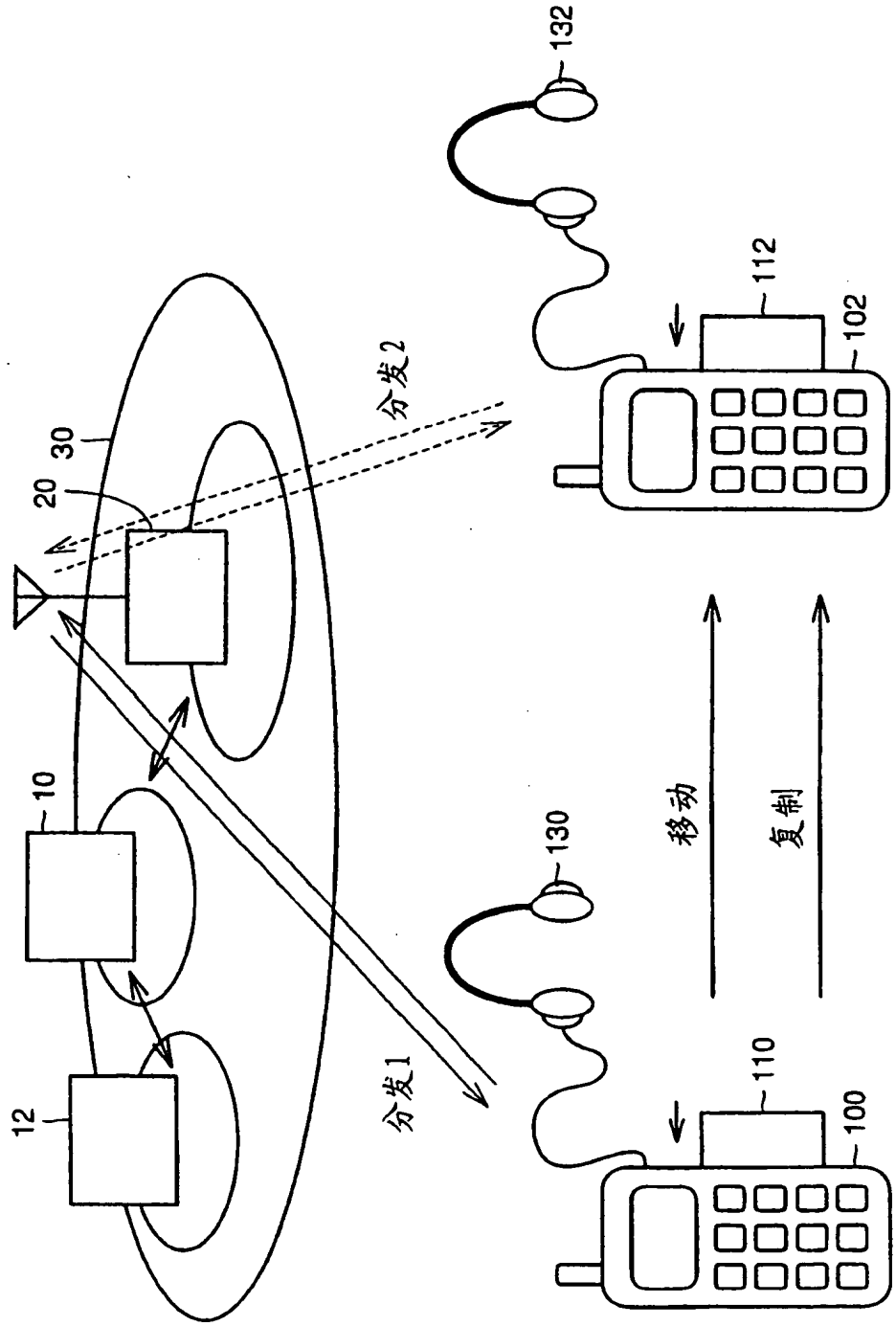


图 1

	记号	属性	特性	
存储插件内管理密钥	Kmedia(n)	秘密解密密钥	媒体固有	具有按存储插件的种类固有的信息
	Kcard(n)	秘密解密密钥		按各存储插件而不同
	KPcard(n)	公开加密密钥		与Kcard(n)成对 根据KPcard(n)加密后的数据能够用Kcard(n)解密
存储插件外管理密钥	KPmedia(n)	公开加密密钥	媒体固有	与Kmedia成对 根据KPmedia加密后的数据能够用Kmedia解密
	Ks	公用密钥	对话固有	每逢通信（例：每次访问）时产生，在分发服务器、便携式电话机管理
分发数据	Kc	公用密钥	许可Key	加密内容数据的解密密钥
	License-ID	再生相关信息		例：曲目的特定信息 再生次数的限制信息
	User-ID	识别接收者的信息		例：电话号码
	Dc	内容数据		例：音乐
	[Dc]Kc	加密内容数据		根据公用密钥Kc加密后的内容数据

图 2

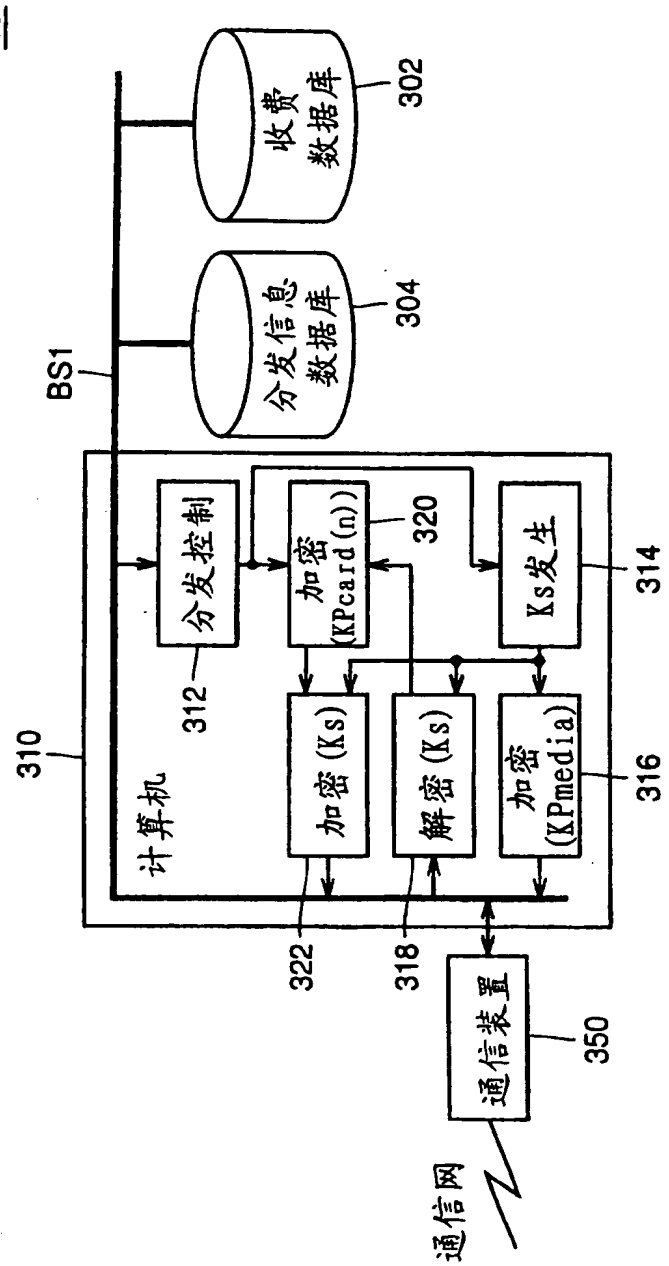

10
收费数据库
302
分发信息数据库
304
BS1
计算机
310
分发控制
312
加密(KPcard(n))
320
Ks发生
314
加密(Ks)
322
解密(Ks)
318
加密(KPmedia)
316
通信装置
350
通信网

图 3

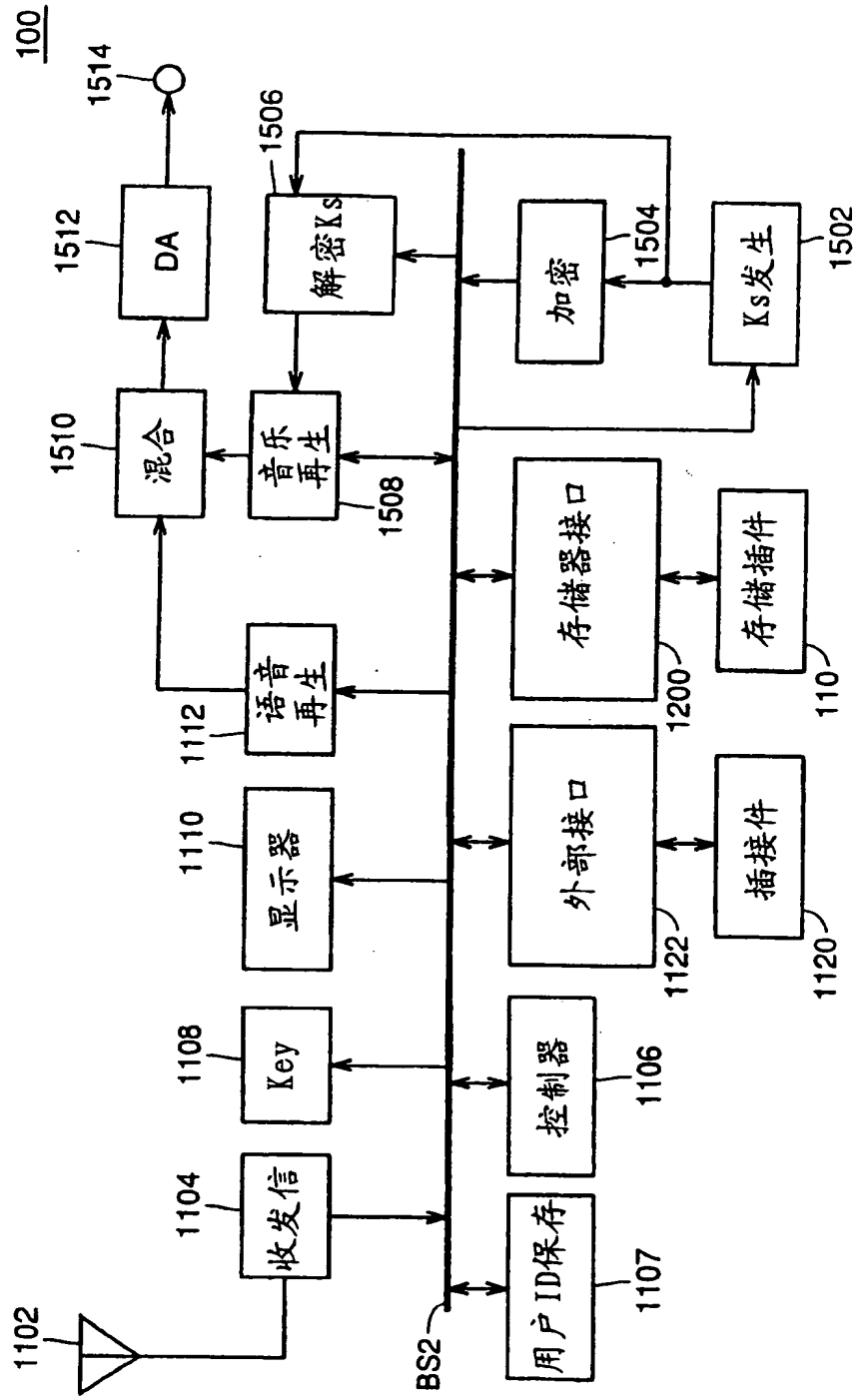

100
1514
1506
1512
DA
解密Ks
加密
1504
Ks发生
1502
1510
混合
音乐再生
1508
存储器接口
存储插件
1200
110
1112
语音再生
1110
显示器
外部接口
插接件
1122
1120
1108
Key
控制器
1106
1104
收发信
用户ID保存
1107
1102
BS2

图 4

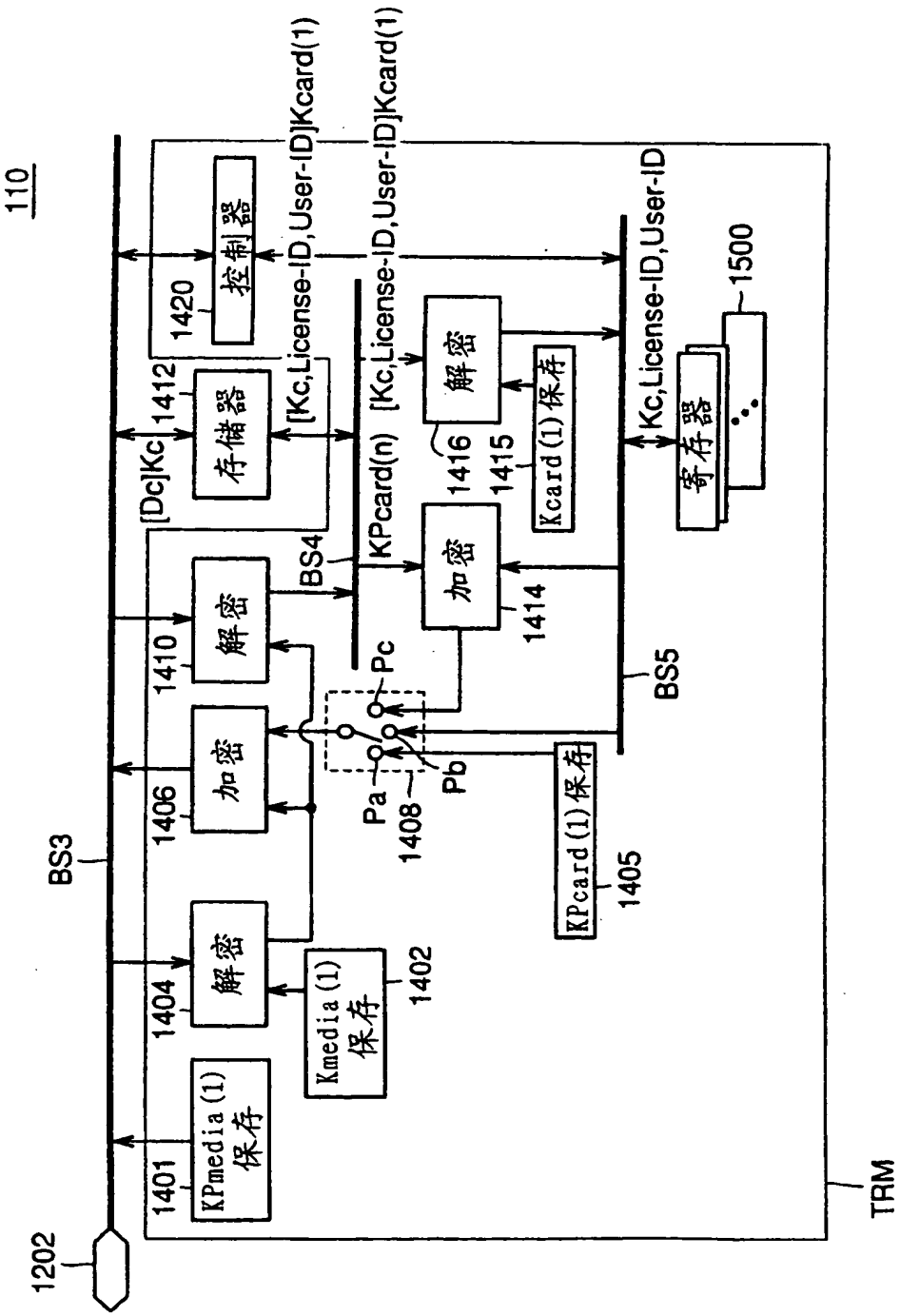

110
BS3
BS4
BS5
TRM
1202
1401
KPmedia(1)保存
1402
Kmedia(1)保存
1404
解密
1406
加密
1408
Pa
Pb
Pc
1410
解密
1412
存储器
1414
加密
1415
Kcard(1)保存
1416
解密
1420
控制器
1405
KPcard(1)保存
1500
寄存器
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
KPcard(n)
[Kc,License-ID,User-ID]Kcard(1)
Kc,License-ID,User-ID

图 5

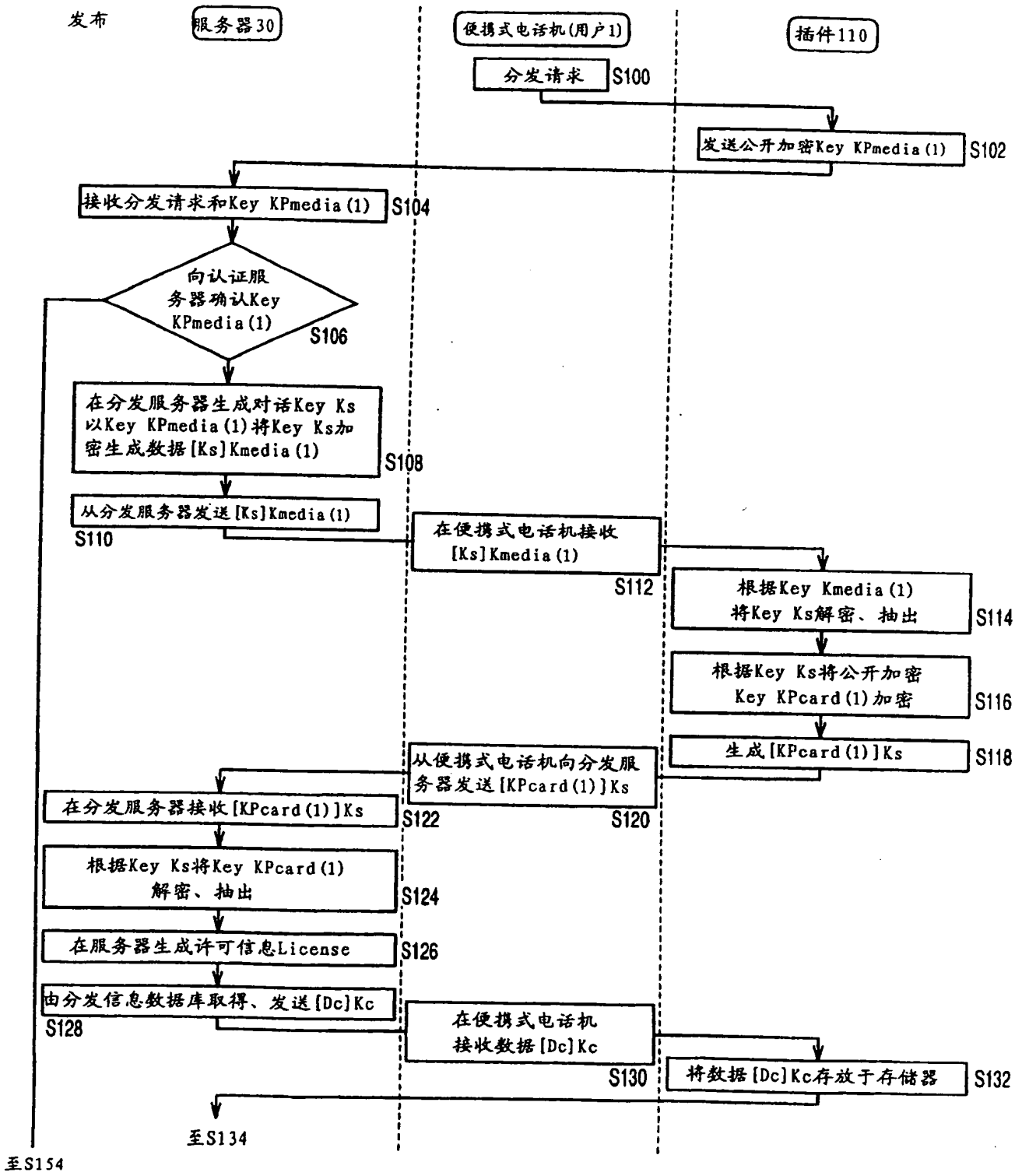

发布
服务器30
便携式电话机(用户1)
插件110
分发请求
S100
发送公开加密Key KPmedia(1)
S102
接收分发请求和Key KPmedia(1)
S104
向认证服务器确认Key KPmedia(1)
S106
在分发服务器生成对话Key Ks以Key KPmedia(1)将Key Ks加密生成数据[Ks]Kmedia(1)
S108
从分发服务器发送[Ks]Kmedia(1)
S110
在便携式电话机接收[Ks]Kmedia(1)
S112
根据Key Kmedia(1)将Key Ks解密、抽出
S114
根据Key Ks将公开加密Key KPcard(1)加密
S116
生成[KPcard(1)]Ks
S118
从便携式电话机向分发服务器发送[KPcard(1)]Ks
S120
在分发服务器接收[KPcard(1)]Ks
S122
根据Key Ks将Key KPcard(1)解密、抽出
S124
在服务器生成许可信息License
S126
由分发信息数据库取得、发送[Dc]Kc
S128
在便携式电话机接收数据[Dc]Kc
S130
将数据[Dc]Kc存放于存储器
S132
至S134
至S154

图 6

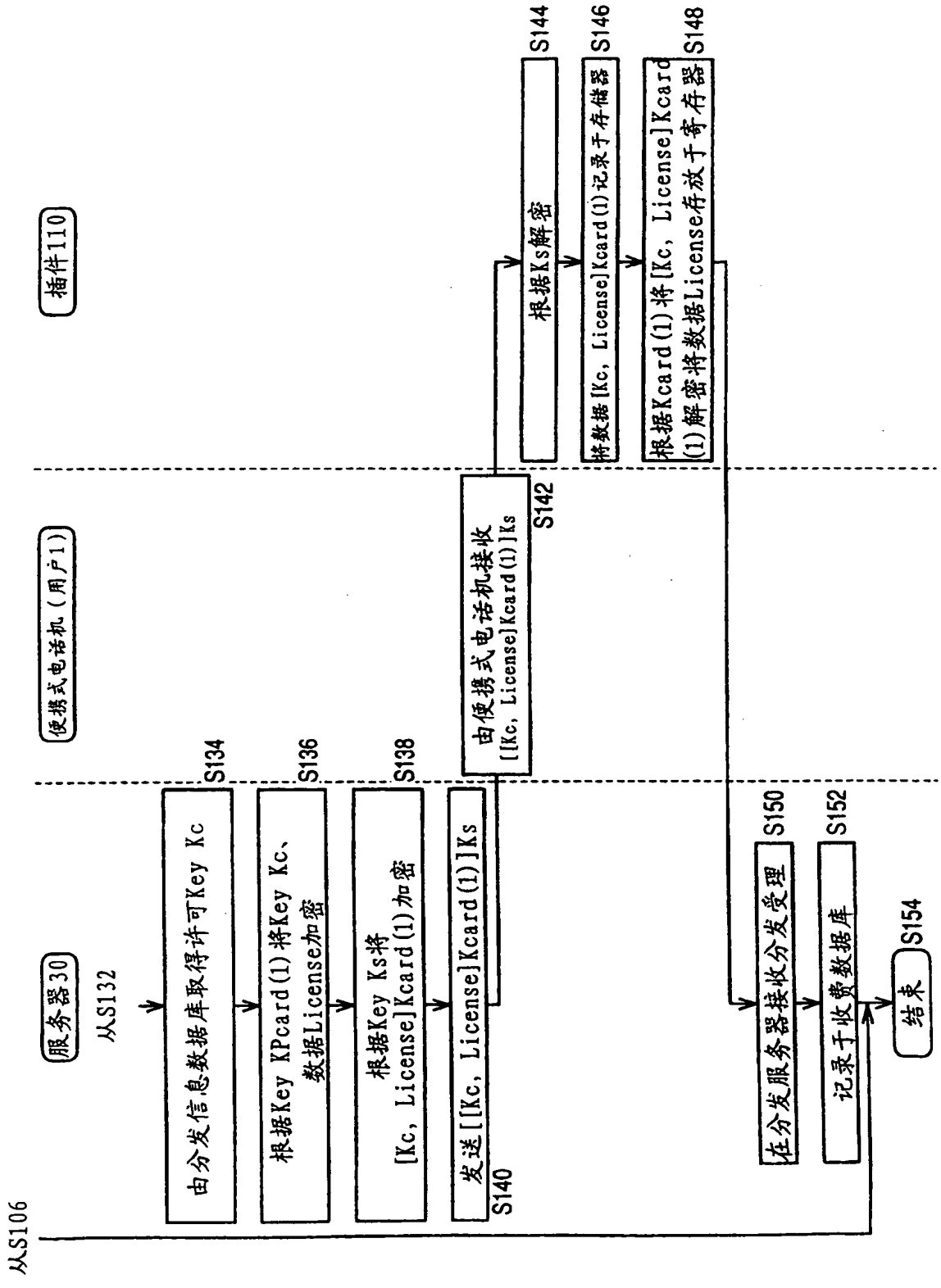

从S106
服务器30
从S132
便携式电话机（用户1）
插件110
由分发信息数据库取得许可Key Kc
S134
根据Key KPcard(1)将Key Kc、数据License加密
S136
根据Key Ks将[Kc, License]Kcard(1)加密
S138
发送[[Kc, License]Kcard(1)]Ks
S140
由便携式电话机接收[[Kc, License]Kcard(1)]Ks
S142
根据Ks解密
S144
将数据[Kc, License]Kcard(1)记录于存储器
S146
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S148
在分发服务器接收分发受理
S150
记录于收费数据库
S152
结束
S154

图 7

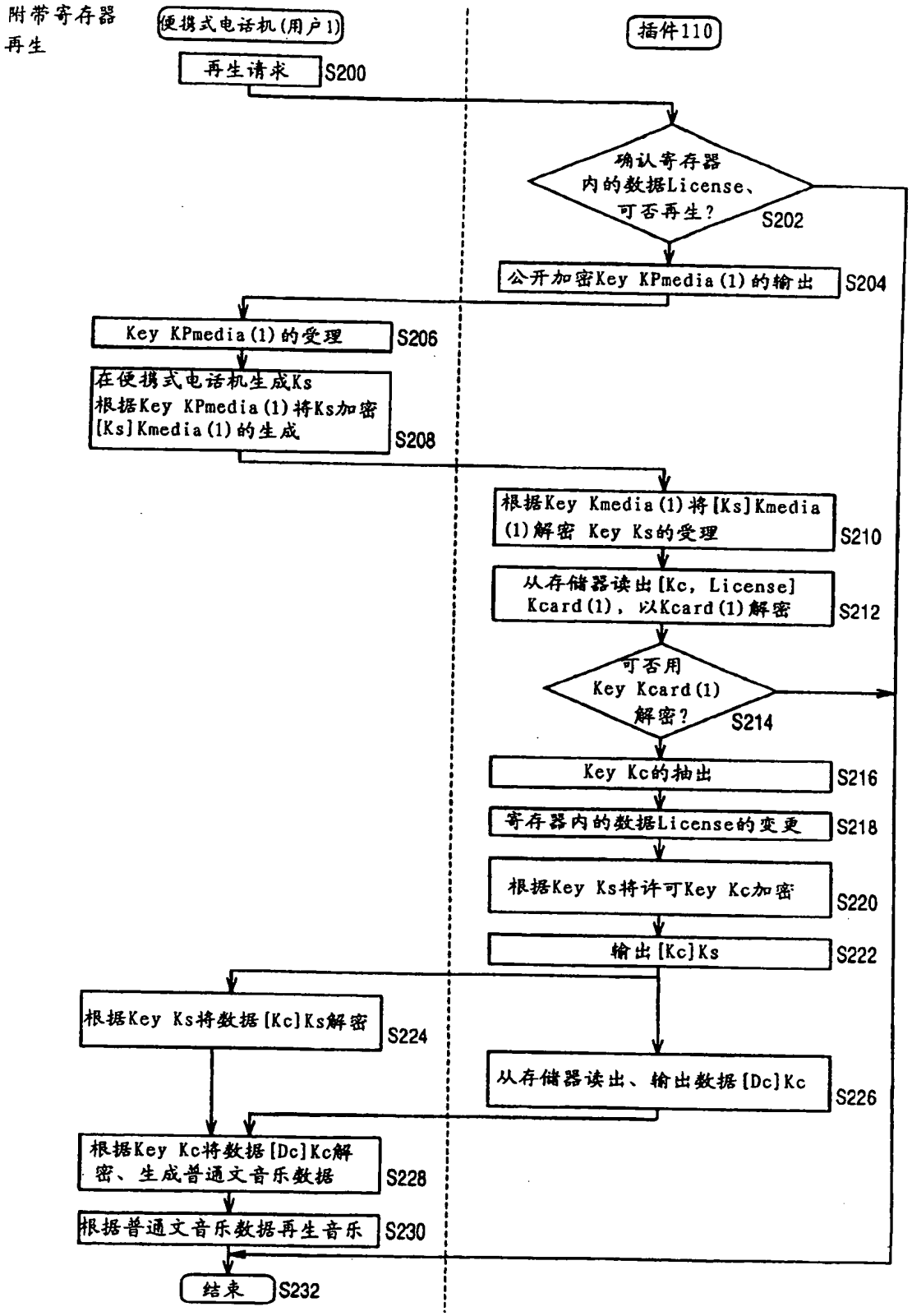

附带寄存器
再生
便携式电话机(用户1)
插件110
再生请求
S200
确认寄存器
内的数据License、
可否再生?
S202
公开加密Key KPmedia(1)的输出
S204
Key KPmedia(1)的受理
S206
在便携式电话机生成Ks
根据Key KPmedia(1)将Ks加密
[Ks]Kmedia(1)的生成
S208
根据Key Kmedia(1)将[Ks]Kmedia
(1)解密 Key Ks的受理
S210
从存储器读出[Kc, License]
Kcard(1), 以Kcard(1)解密
S212
可否用
Key Kcard(1)
解密?
S214
Key Kc的抽出
S216
寄存器内的数据License的变更
S218
根据Key Ks将许可Key Kc加密
S220
输出[Kc]Ks
S222
根据Key Ks将数据[Kc]Ks解密
S224
从存储器读出、输出数据[Dc]Kc
S226
根据Key Kc将数据[Dc]Kc解
密、生成普通文音乐数据
S228
根据普通文音乐数据再生音乐
S230
结束
S232

图 8

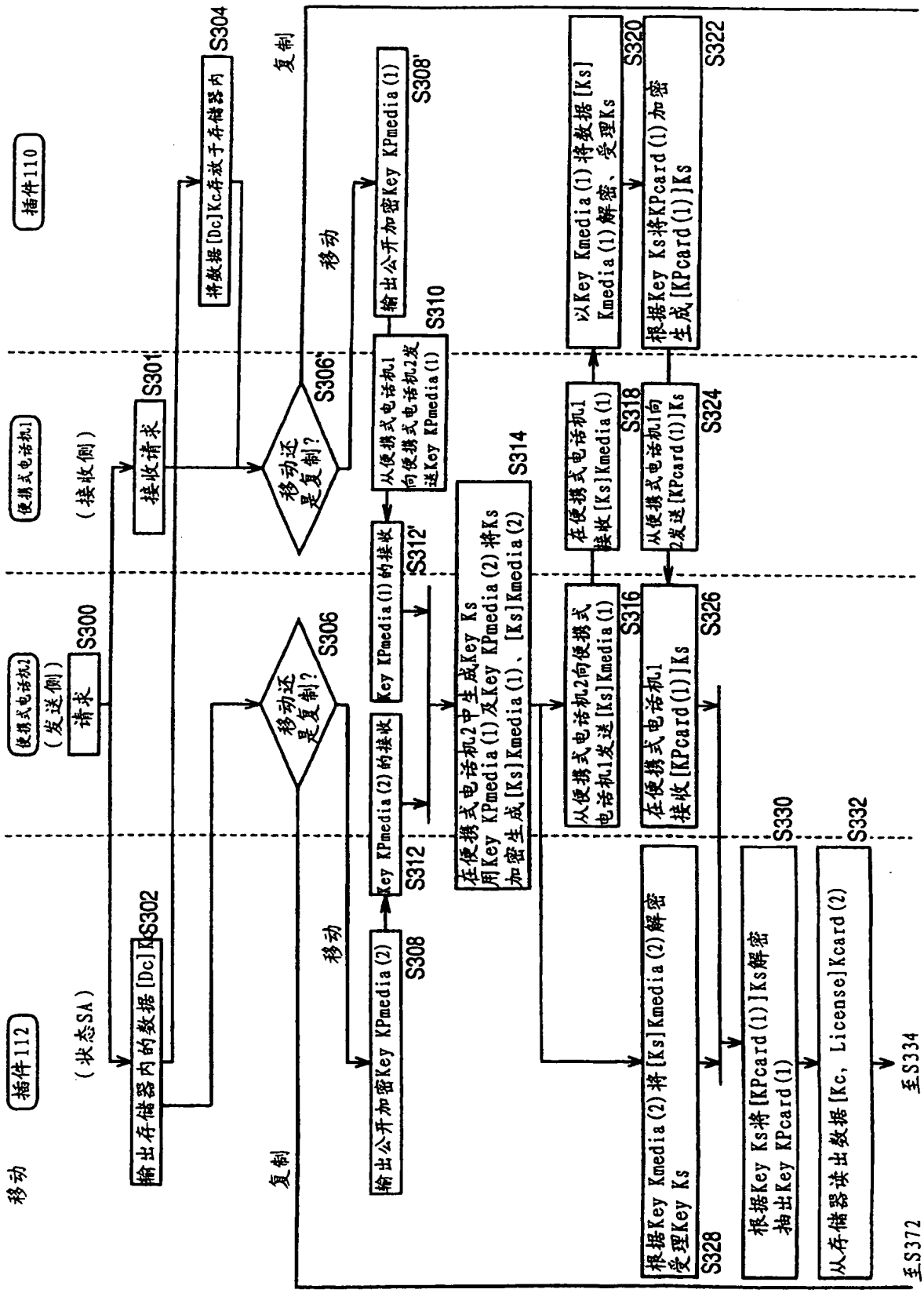

移动
插件112
便携式电话机2
（发送侧）
便携式电话机1
（接收侧）
插件110
（状态SA）
请求
S300
接收请求
S301
输出存储器内的数据[Dc]Kc
S302
将数据[Dc]Kc存放于存储器内
S304
复制
移动
移动还是复制?
S306
S306'
输出公开加密Key KPmedia(2)
S308
输出公开加密Key KPmedia(1)
S308'
Key KPmedia(2)的接收
S312
Key KPmedia(1)的接收
S312'
从便携式电话机1向便携式电话机2发送Key KPmedia(1)
S310
在便携式电话机2中生成Key Ks
用Key KPmedia(1)及Key KPmedia(2)将Ks
加密生成[Ks]Kmedia(1)、[Ks]Kmedia(2)
S314
从便携式电话机2向便携式电话机1发送[Ks]Kmedia(1)
S316
在便携式电话机1接收[Ks]Kmedia(1)
S318
以Key Kmedia(1)将数据[Ks]Kmedia(1)解密、受理Ks
S320
在便携式电话机1接收[KPcard(1)]Ks
S326
从便携式电话机1向便携式电话机2发送[KPcard(1)]Ks
S324
根据Key Ks将KPcard(1)加密生成[KPcard(1)]Ks
S322
根据Key Kmedia(2)将[Ks]Kmedia(2)解密受理Key Ks
S328
根据Key Ks将[KPcard(1)]Ks解密抽出Key KPcard(1)
S330
从存储器读出数据[Kc, License]Kcard(2)
S332
至S372
至S334

图 9

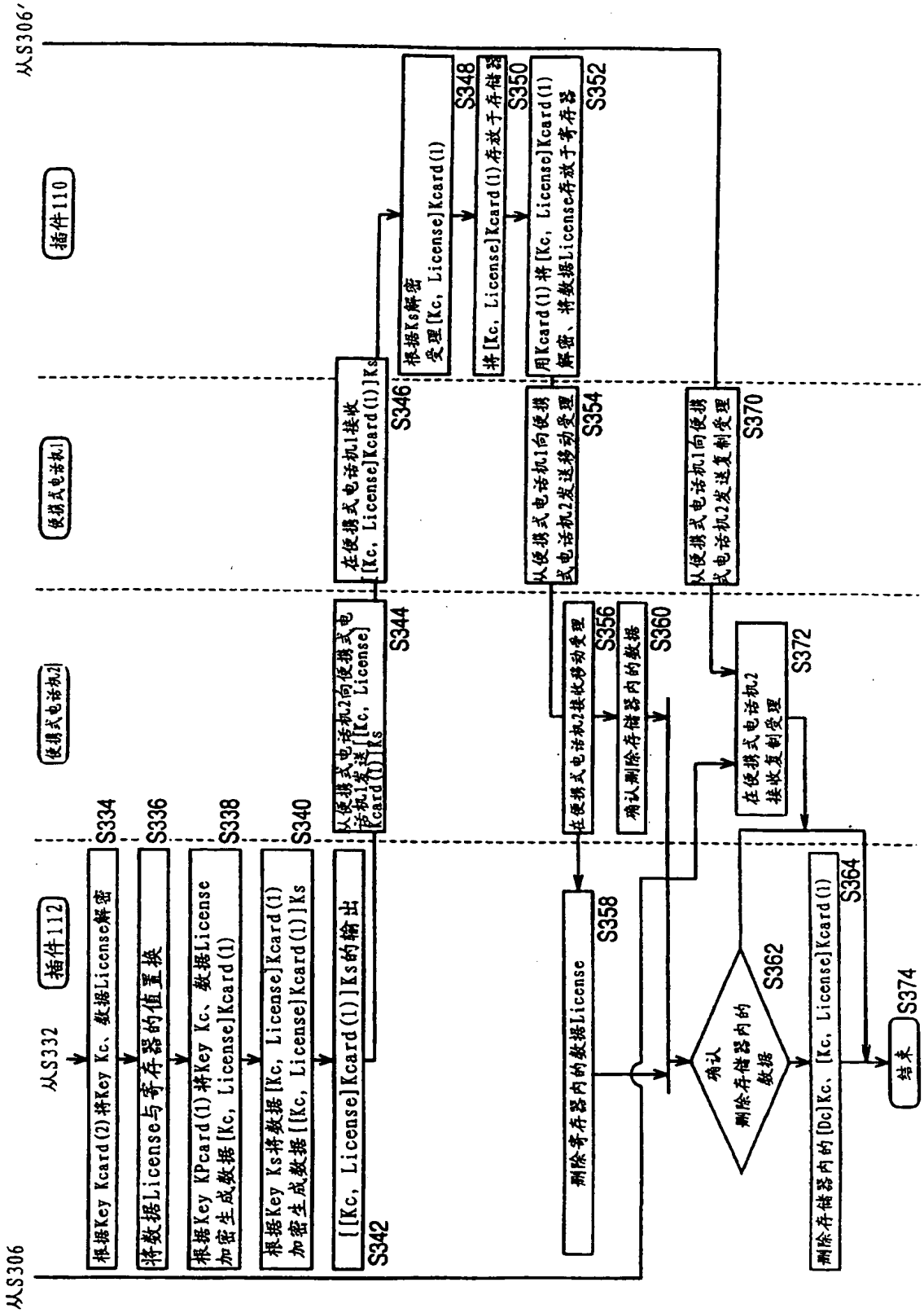

从S306
从S306'
插件112
便携式电话机2
便携式电话机1
插件110
从S332
根据Key Kcard(2)将Key Kc、数据License解密
S334
将数据License与寄存器的值置换
S336
根据Key KPcard(1)将Key Kc、数据License加密生成数据[Kc, License]Kcard(1)
S338
根据Key Ks将数据[Kc, License]Kcard(1)加密生成数据{[Kc, License]Kcard(1)}Ks
S340
{[Kc, License]Kcard(1)}Ks的输出
S342
从便携式电话机2向便携式电话机1发送{[Kc, License]Kcard(1)}Ks
S344
在便携式电话机1接收[Kc, License]Kcard(1)}Ks
S346
根据Ks解密处理[Kc, License]Kcard(1)
S348
将[Kc, License]Kcard(1)存放于存储器
S350
用Kcard(1)将[Kc, License]Kcard(1)解密、将数据License存放于寄存器
S352
从便携式电话机1向便携式电话机2发送移动受理
S354
在便携式电话机2接收移动受理
S356
确认删除存储器内的数据
S360
从便携式电话机1向便携式电话机2发送复制受理
S370
在便携式电话机2接收复制受理
S372
删除寄存器内的数据License
S358
确认删除存储器内的数据
S362
删除存储器内的[Dc]Kc、{[Kc, License]Kcard(1)
S364
结束
S374

图 10

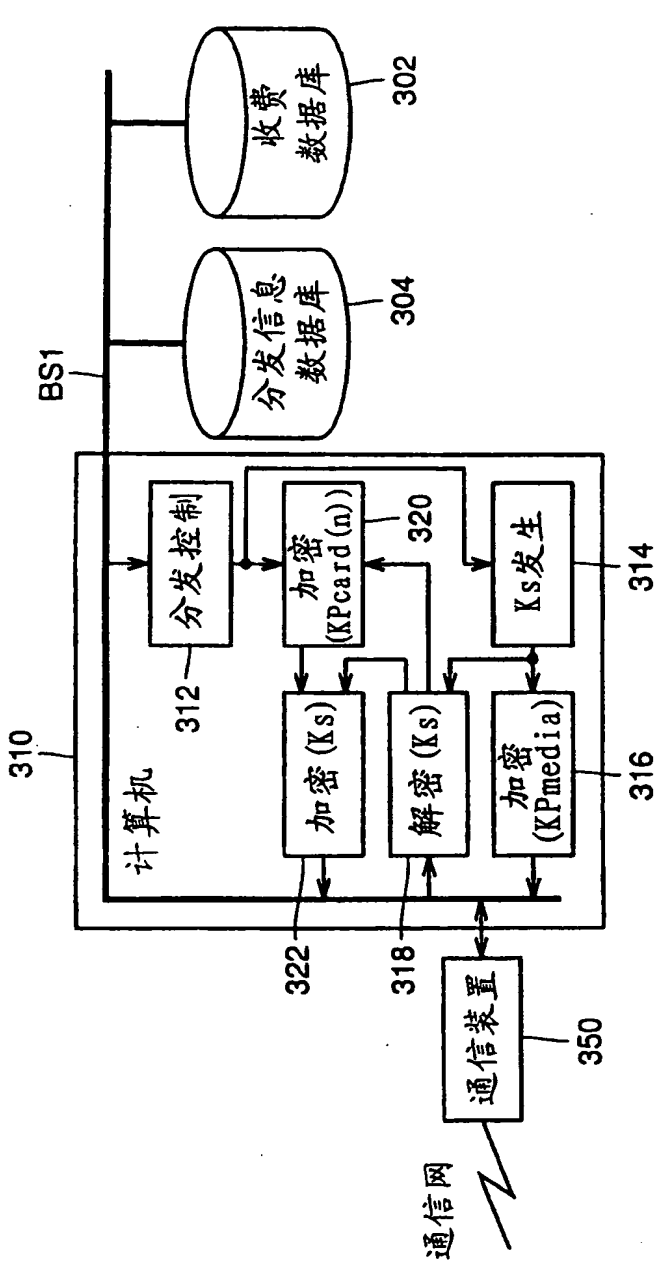

11
收费数据库
302
分发信息数据库
304
BS1
计算机
310
分发控制
312
加密(KPcard(n))
320
Ks发生
314
加密(Ks)
322
解密(Ks)
318
加密(KPmedia)
316
通信装置
350
通信网

图 11

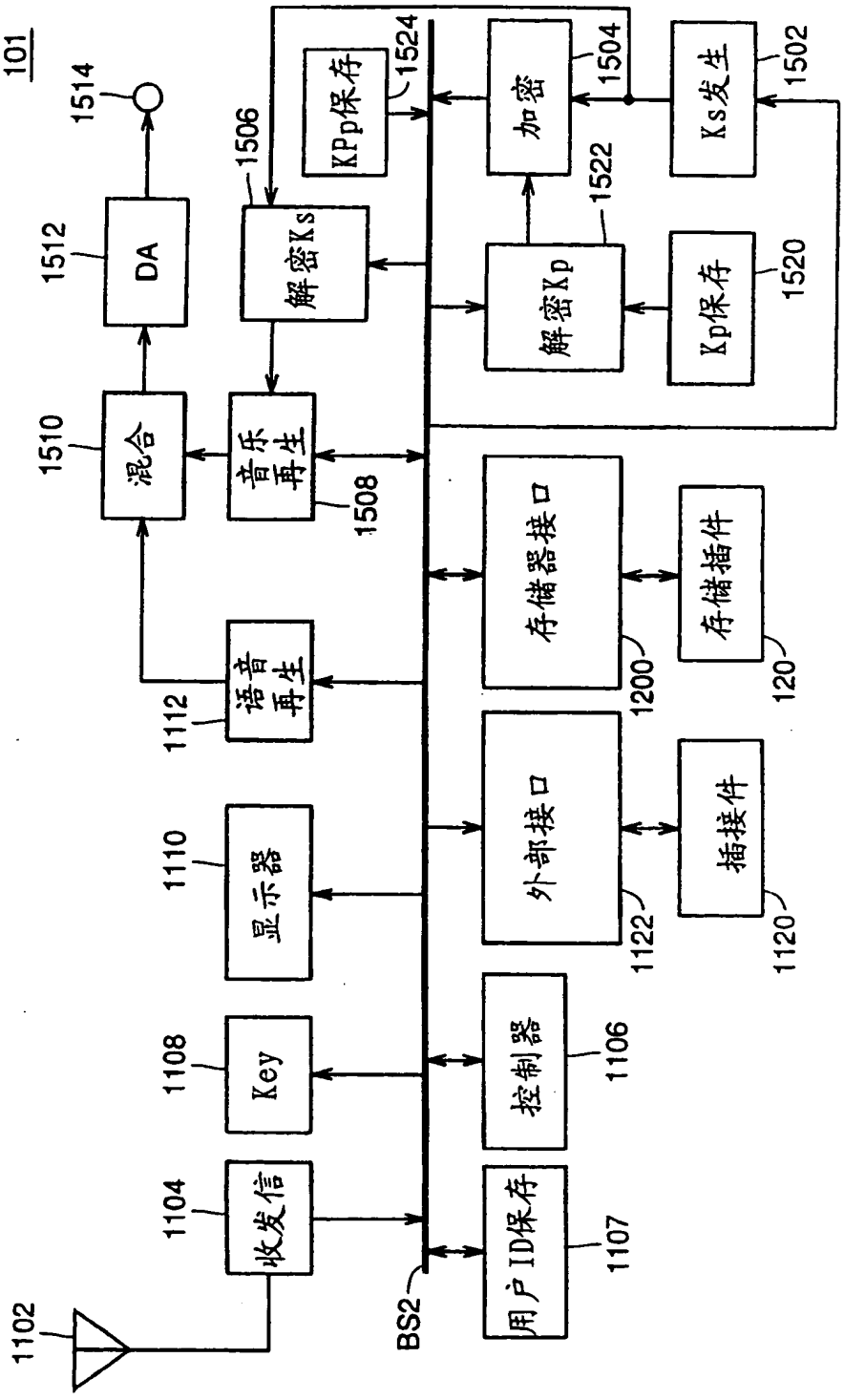

101
1514
1512
DA
1510
混合
1506
解密Ks
KPp保存
1524
加密
1504
Ks发生
1502
1522
解密Kp
Kp保存
1520
音乐再生
1508
存储器接口
1200
存储插件
120
1112
语音再生
1110
显示器
外部接口
1122
插接件
1120
1108
Key
控制器
1106
1104
收发信
用户ID保存
1107
1102
BS2

图 12

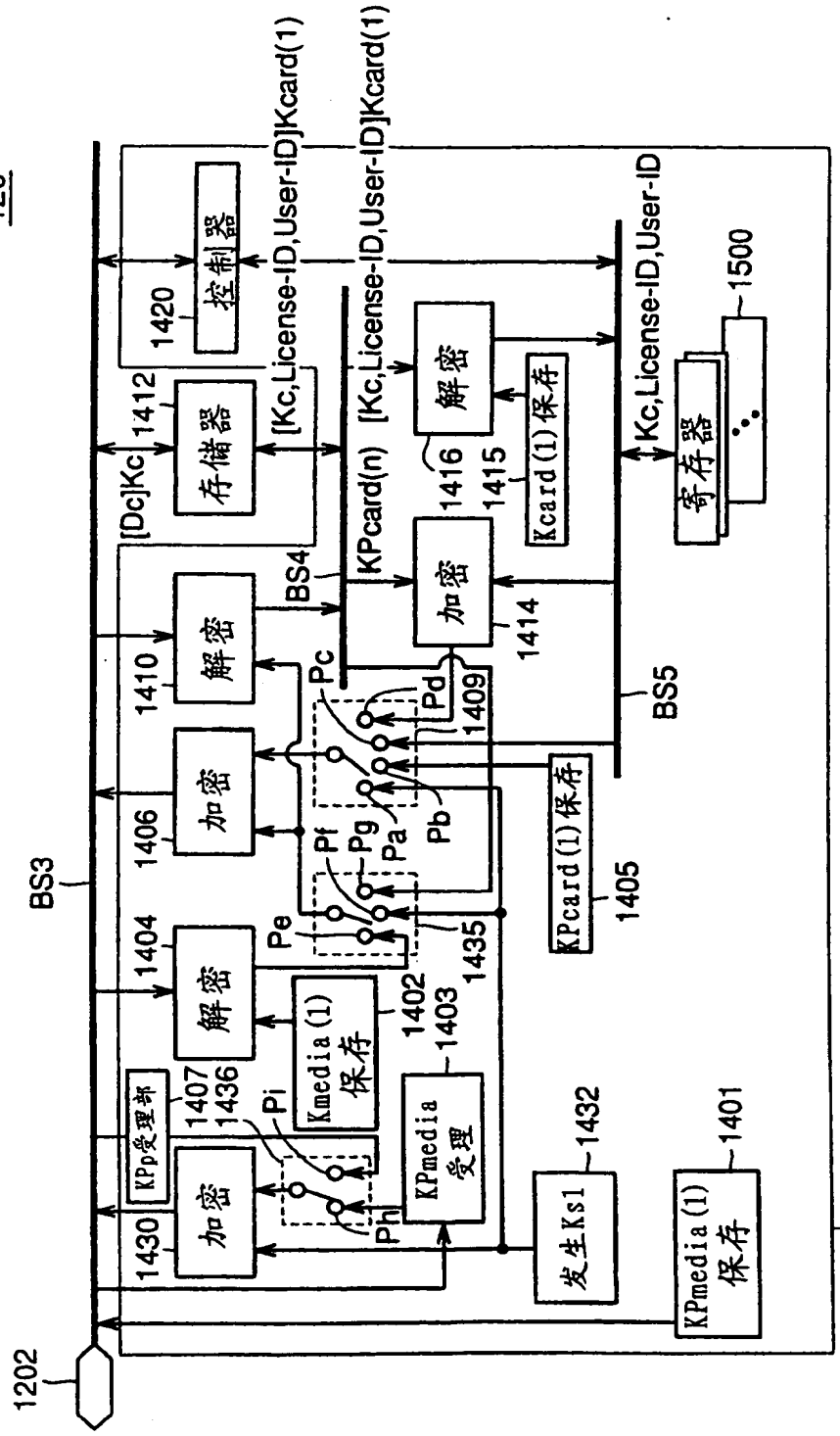

120
1202
BS3
BS4
BS5
TRM
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
Kc,License-ID,User-ID
KPcard(n)
1420
控制器
1412
存储器
1410
解密
1406
加密
1404
解密
1407
1436
KPp受理部
1430
加密
1402
1403
Kmedia(1)保存
KPmedia受理
1432
发生Ks1
1401
KPmedia(1)保存
1405
KPcard(1)保存
1409
1414
加密
1416
1415
解密
Kcard(1)保存
1500
寄存器
Pc
Pd
Pe
Pf
Pg
Pa
Pb
Pi
Ph
1435

图 13

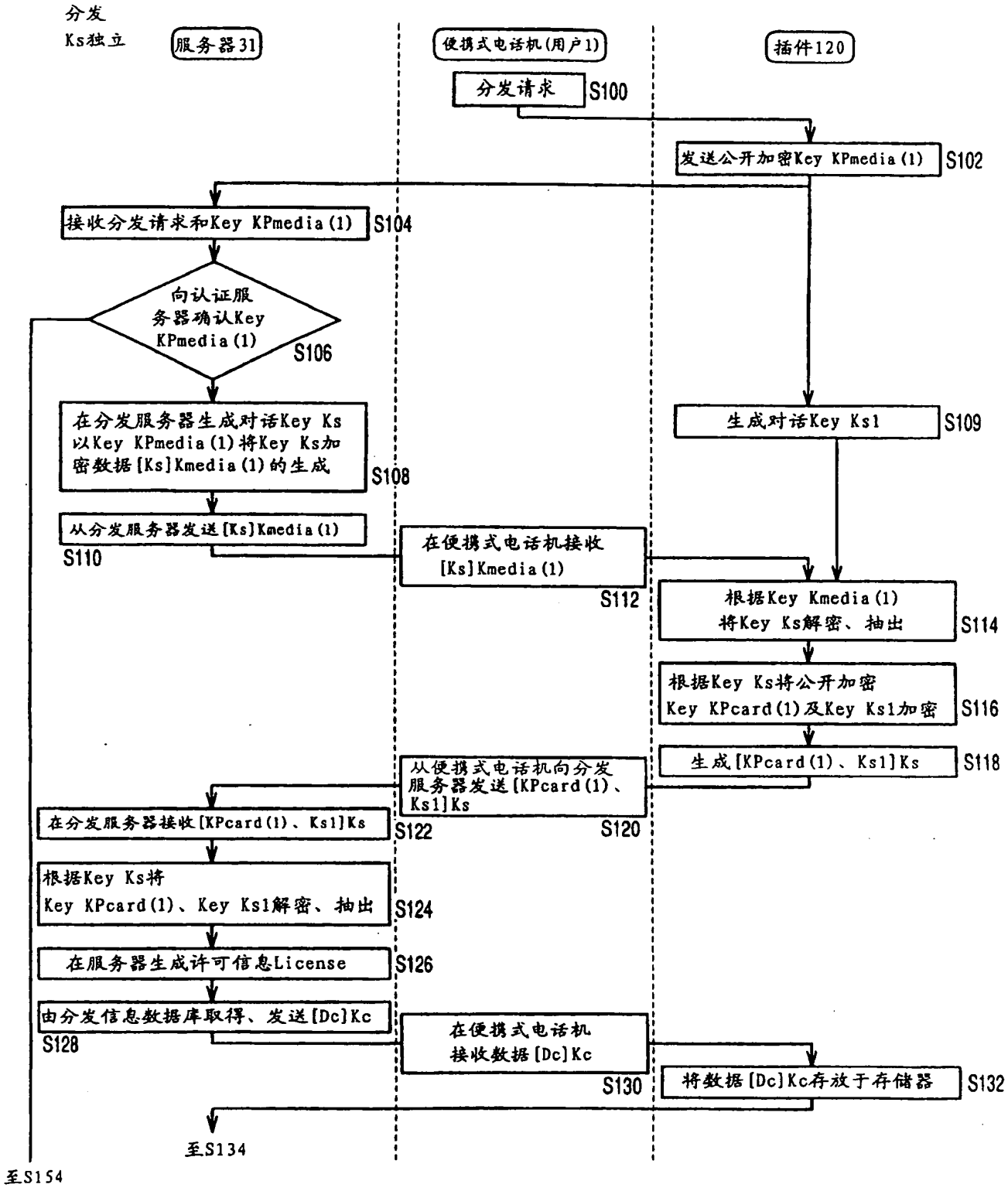

分发
Ks独立
服务器31
便携式电话机(用户1)
插件120
分发请求
S100
发送公开加密Key KPmedia(1)
S102
接收分发请求和Key KPmedia(1)
S104
向认证服务器确认Key KPmedia(1)
S106
在分发服务器生成对话Key Ks以Key KPmedia(1)将Key Ks加密数据[Ks]Kmedia(1)的生成
S108
生成对话Key Ks1
S109
从分发服务器发送[Ks]Kmedia(1)
S110
在便携式电话机接收[Ks]Kmedia(1)
S112
根据Key Kmedia(1)将Key Ks解密、抽出
S114
根据Key Ks将公开加密Key KPcard(1)及Key Ks1加密
S116
生成[KPcard(1)、Ks1]Ks
S118
从便携式电话机向分发服务器发送[KPcard(1)、Ks1]Ks
S120
在分发服务器接收[KPcard(1)、Ks1]Ks
S122
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S124
在服务器生成许可信息License
S126
由分发信息数据库取得、发送[Dc]Kc
S128
在便携式电话机接收数据[Dc]Kc
S130
将数据[Dc]Kc存放于存储器
S132
至S134
至S154

图 14

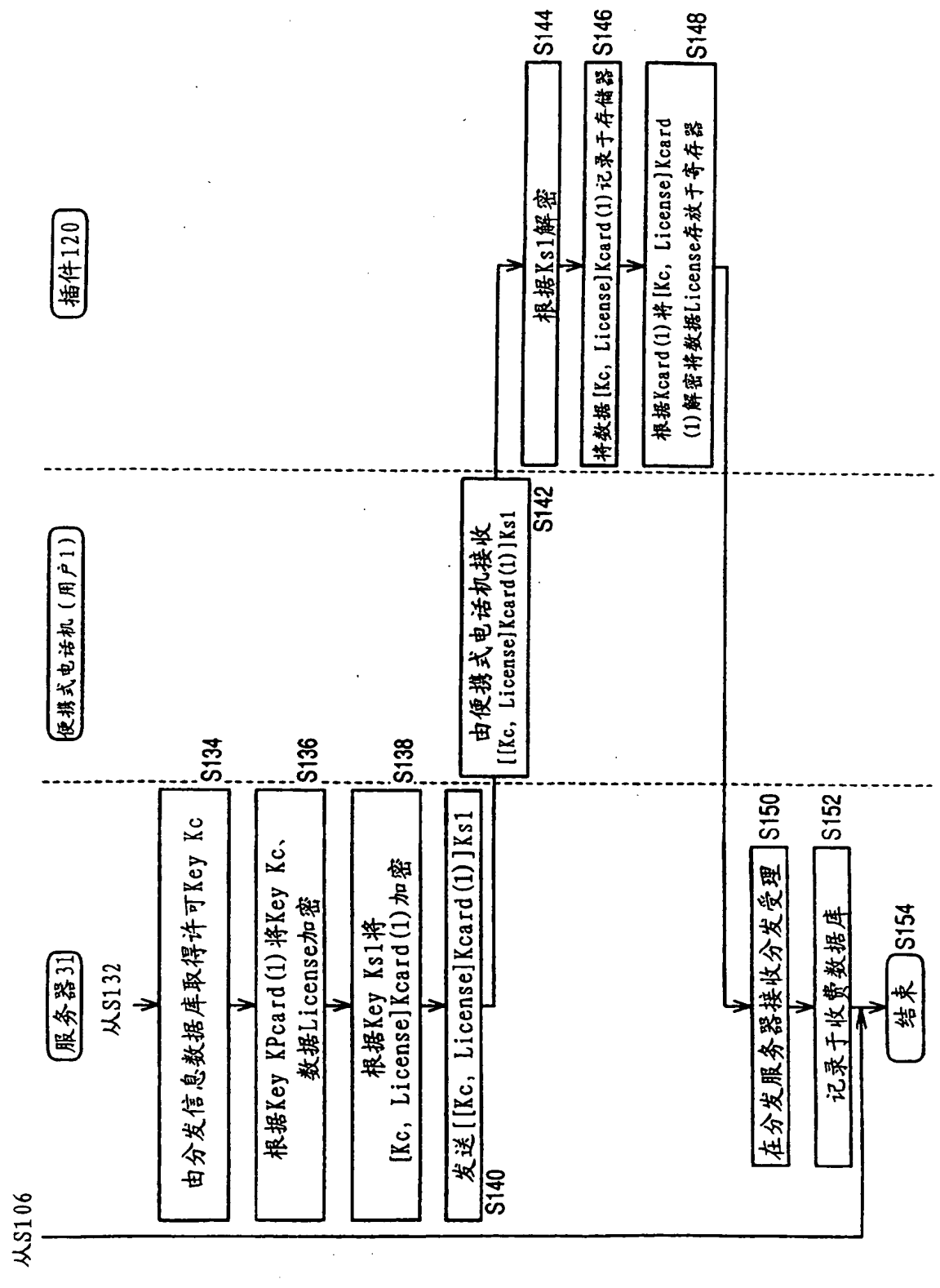

从S106
服务器31
从S132
由分发信息数据库取得许可Key Kc
S134
根据Key KPcard(1)将Key Kc、数据License加密
S136
根据Key Ks1将[Kc, License]Kcard(1)加密
S138
发送[[Kc, License]Kcard(1)]Ks1
S140
便携式电话机(用户1)
由便携式电话机接收[[Kc, License]Kcard(1)]Ks1
S142
插件120
根据Ks1解密
S144
将数据[Kc, License]Kcard(1)记录于存储器
S146
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S148
在分发服务器接收分发受理
S150
记录于收费数据库
S152
结束
S154

图 15

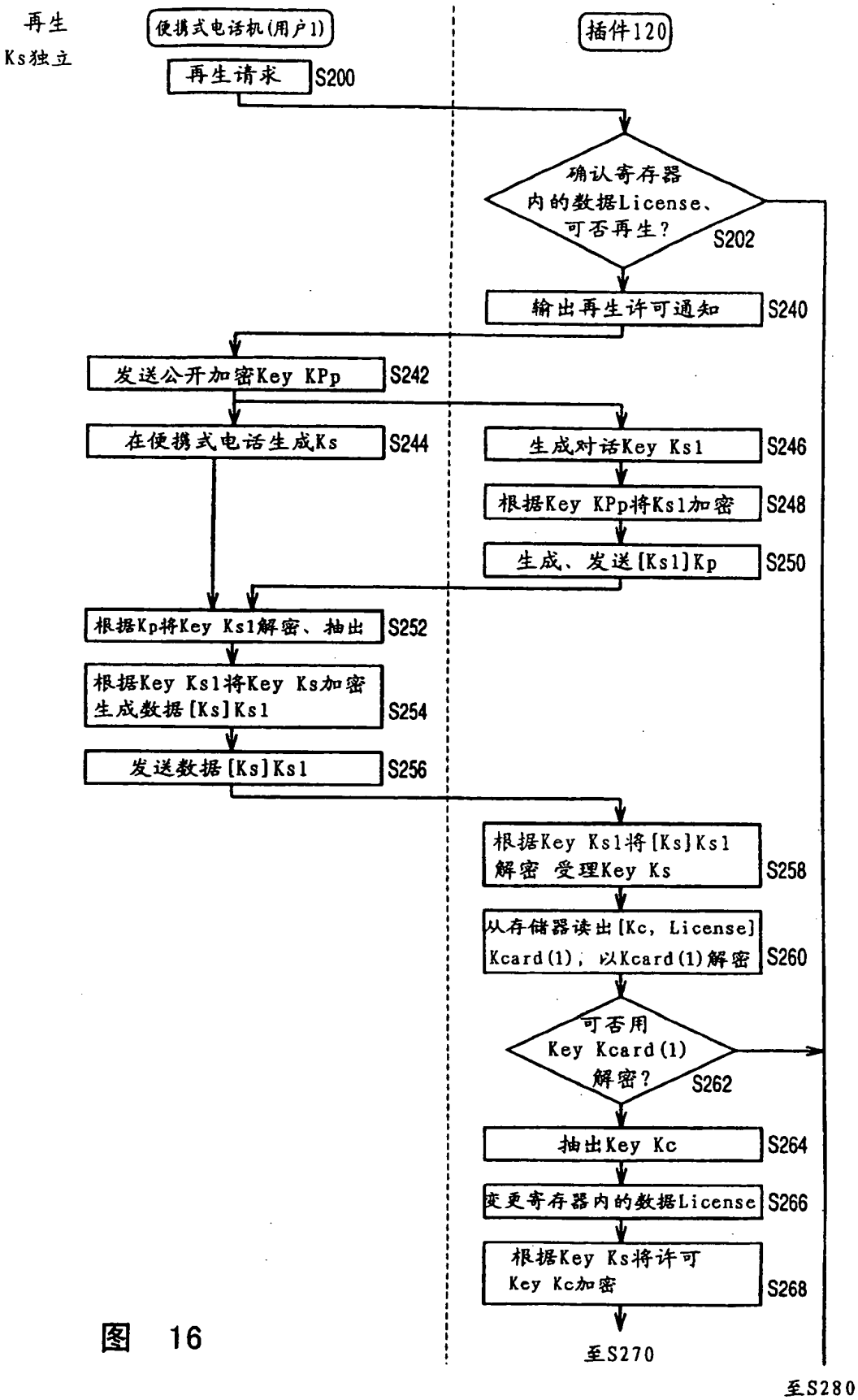

再生
Ks独立
便携式电话机(用户1)
插件120
再生请求 S200
确认寄存器内的数据License、可否再生? S202
输出再生许可通知 S240
发送公开加密Key KPp S242
在便携式电话生成Ks S244
生成对话Key Ks1 S246
根据Key KPp将Ks1加密 S248
生成、发送[Ks1]Kp S250
根据Kp将Key Ks1解密、抽出 S252
根据Key Ks1将Key Ks加密生成数据[Ks]Ks1 S254
发送数据[Ks]Ks1 S256
根据Key Ks1将[Ks]Ks1解密 受理Key Ks S258
从存储器读出[Kc, License]Kcard(1), 以Kcard(1)解密 S260
可否用Key Kcard(1)解密? S262
抽出Key Kc S264
变更寄存器内的数据License S266
根据Key Ks将许可Key Kc加密 S268
至S270
至S280

图 16

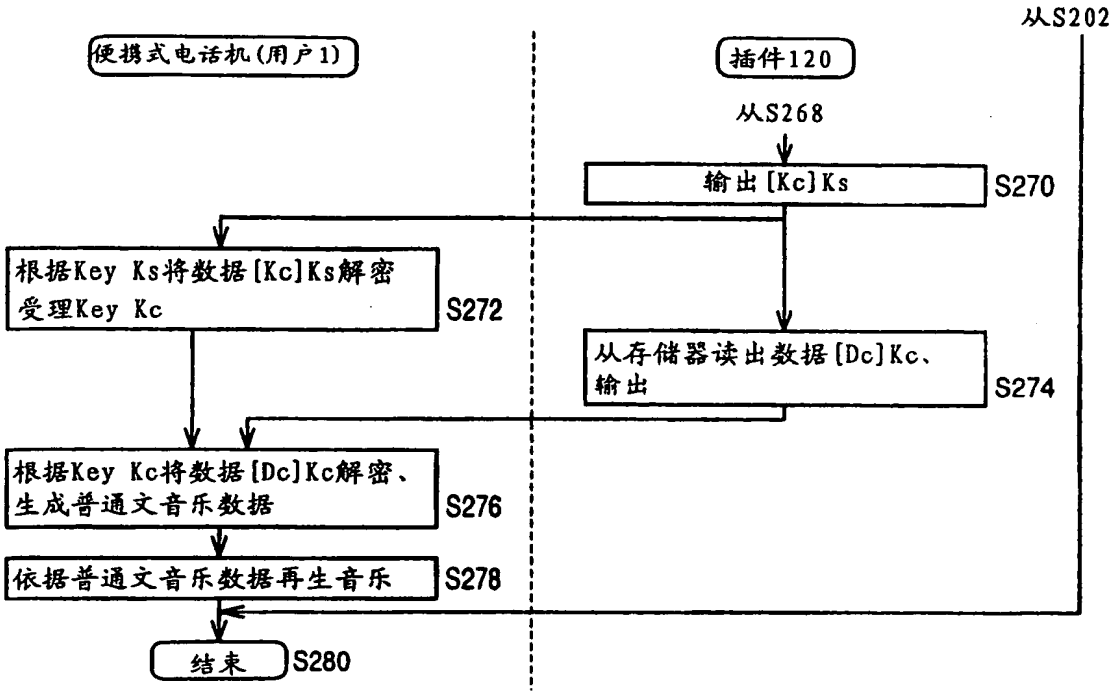

从S202
便携式电话机(用户1)
插件120
从S268
输出[Kc]Ks
S270
根据Key Ks将数据[Kc]Ks解密
受理Key Kc
S272
从存储器读出数据[Dc]Kc、
输出
S274
根据Key Kc将数据[Dc]Kc解密、
生成普通文音乐数据
S276
依据普通文音乐数据再生音乐
S278
结束
S280

图 17

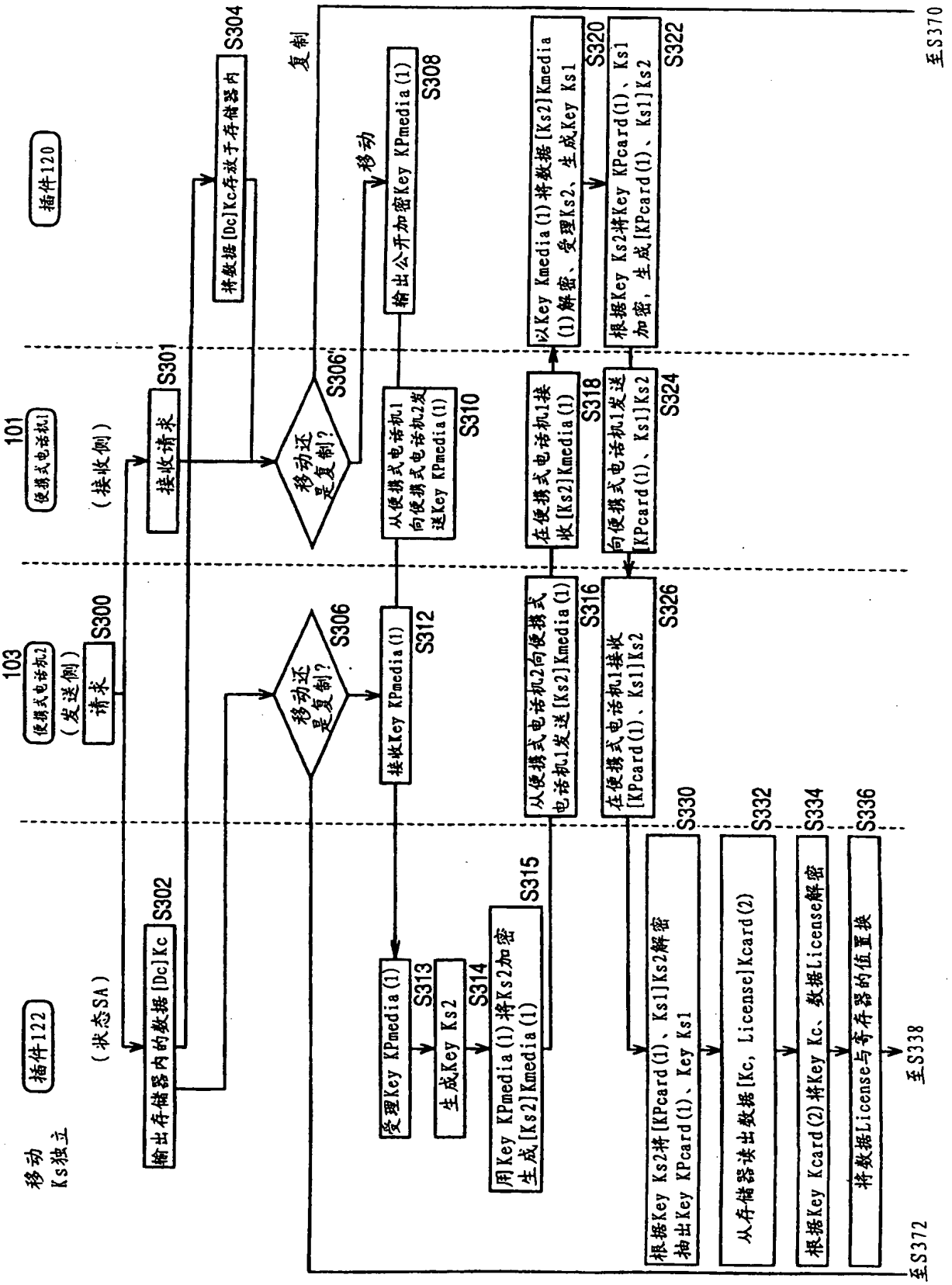

移动
Ks独立
插件122
(状态SA)
103
便携式电话机2
(发送侧)
请求
S300
输出存储器内的数据[Dc]Kc
S302
插件120
101
便携式电话机1
(接收侧)
接收请求
S301
将数据[Dc]Kc存放于存储器内
S304
移动还是复制?
S306
复制
移动
S306'
输出公开加密Key KPmedia(1)
S308
从便携式电话机1向便携式电话机2发送Key KPmedia(1)
S310
移动还是复制?
S306
接收Key KPmedia(1)
S312
受理Key KPmedia(1)
S313
生成Key Ks2
S314
用Key KPmedia(1)将Ks2加密生成[Ks2]Kmedia(1)
S315
从便携式电话机2向便携式电话机1发送[Ks2]Kmedia(1)
S316
在便携式电话机1接收[Ks2]Kmedia(1)
S318
以Key Kmedia(1)将数据[Ks2]Kmedia(1)解密、受理Ks2、生成Key Ks1
S320
根据Key Ks2将Key KPcard(1)、Ks1加密,生成[KPcard(1)、Ks1]Ks2
S322
向便携式电话机1发送[KPcard(1)、Ks1]Ks2
S324
在便携式电话机1接收[KPcard(1)、Ks1]Ks2
S326
根据Key Ks2将[KPcard(1)、Ks1]Ks2解密抽出Key KPcard(1)、Key Ks1
S330
从存储器读出数据[Kc, License]Kcard(2)
S332
根据Key Kcard(2)将Key Kc、数据License解密
S334
将数据License与寄存器的值置换
S336
至S338
至S372
至S370

图 18

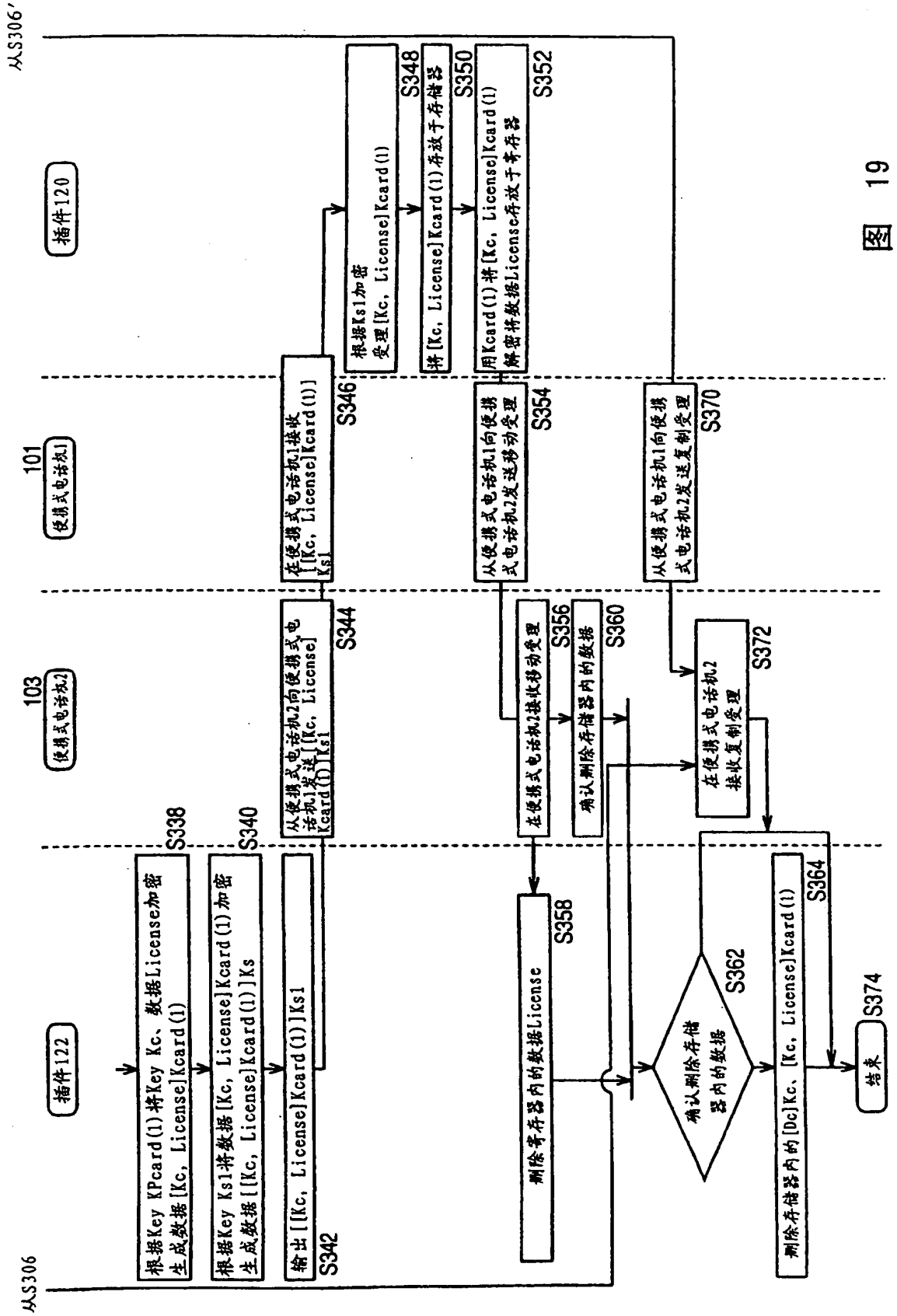

从S306'
插件120
101
便携式电话机1
103
便携式电话机2
插件122
从S306
根据Key KPcard(1)将Key Kc、数据License加密生成数据[Kc, License]Kcard(1)
S338
根据Key Ks1将数据[Kc, License]Kcard(1)加密生成数据[[Kc, License]Kcard(1)]Ks
S340
输出[[Kc, License]Kcard(1)]Ks1
S342
从便携式电话机2向便携式电话机1发送[[Kc, License]Kcard(1)]Ks1
S344
在便携式电话机1接收[[Kc, License]Kcard(1)]Ks1
S346
根据Ks1加密处理[Kc, License]Kcard(1)
S348
将[Kc, License]Kcard(1)存放于存储器
S350
用Kcard(1)将[Kc, License]Kcard(1)解密并获取License存放于存储器
S352
从便携式电话机1向便携式电话机2发送移动处理
S354
在便携式电话机2接收移动处理
S356
确认删除存储器内的数据
S360
删除存储器内的数据License
S358
从便携式电话机1向便携式电话机2发送复制处理
S370
在便携式电话机2接收复制处理
S372
确认删除存储器内的数据
S362
删除存储器内的[Dc]Kc、[Kc, License]Kcard(1)
S364
结束
S374

图 19

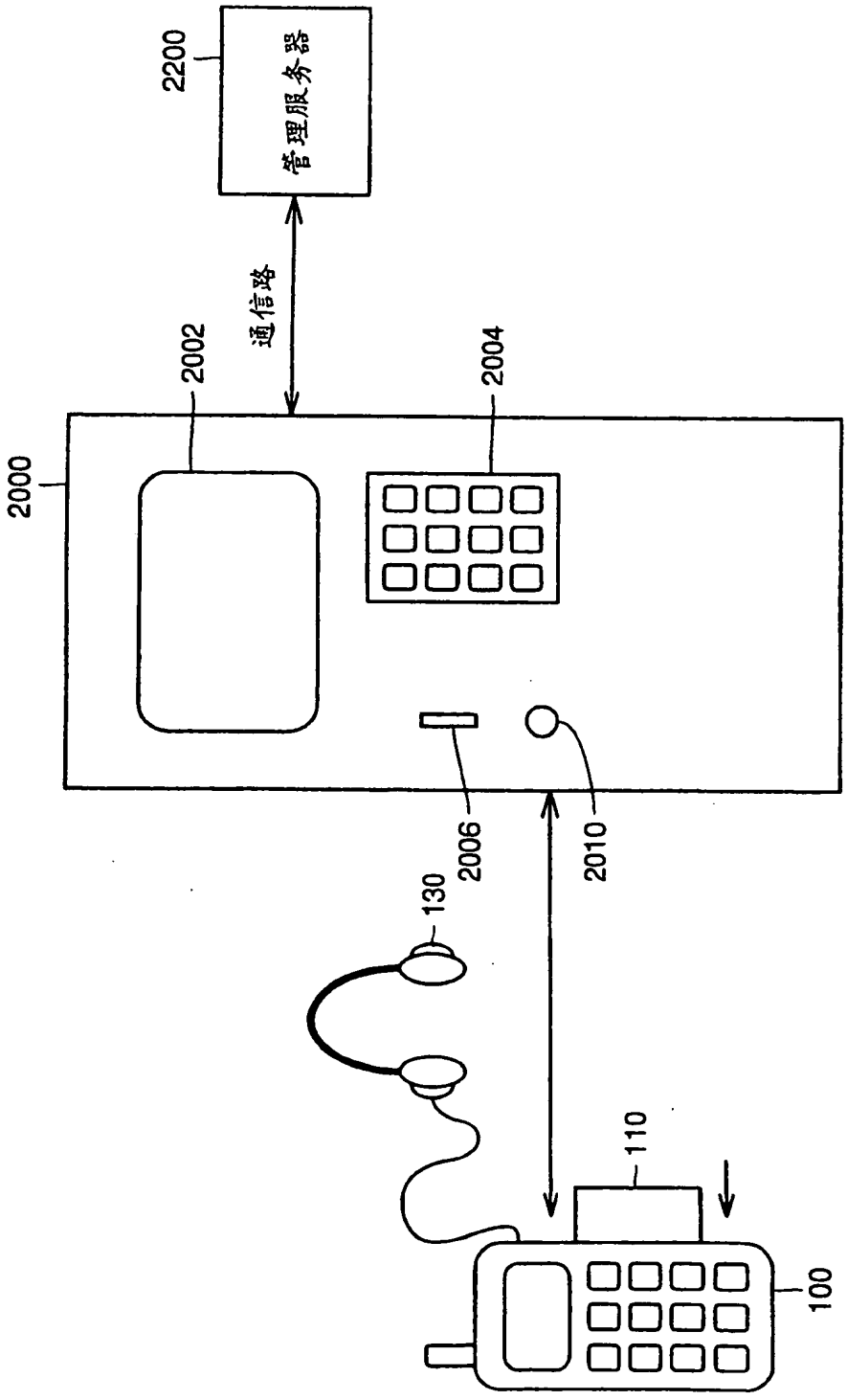


图 20

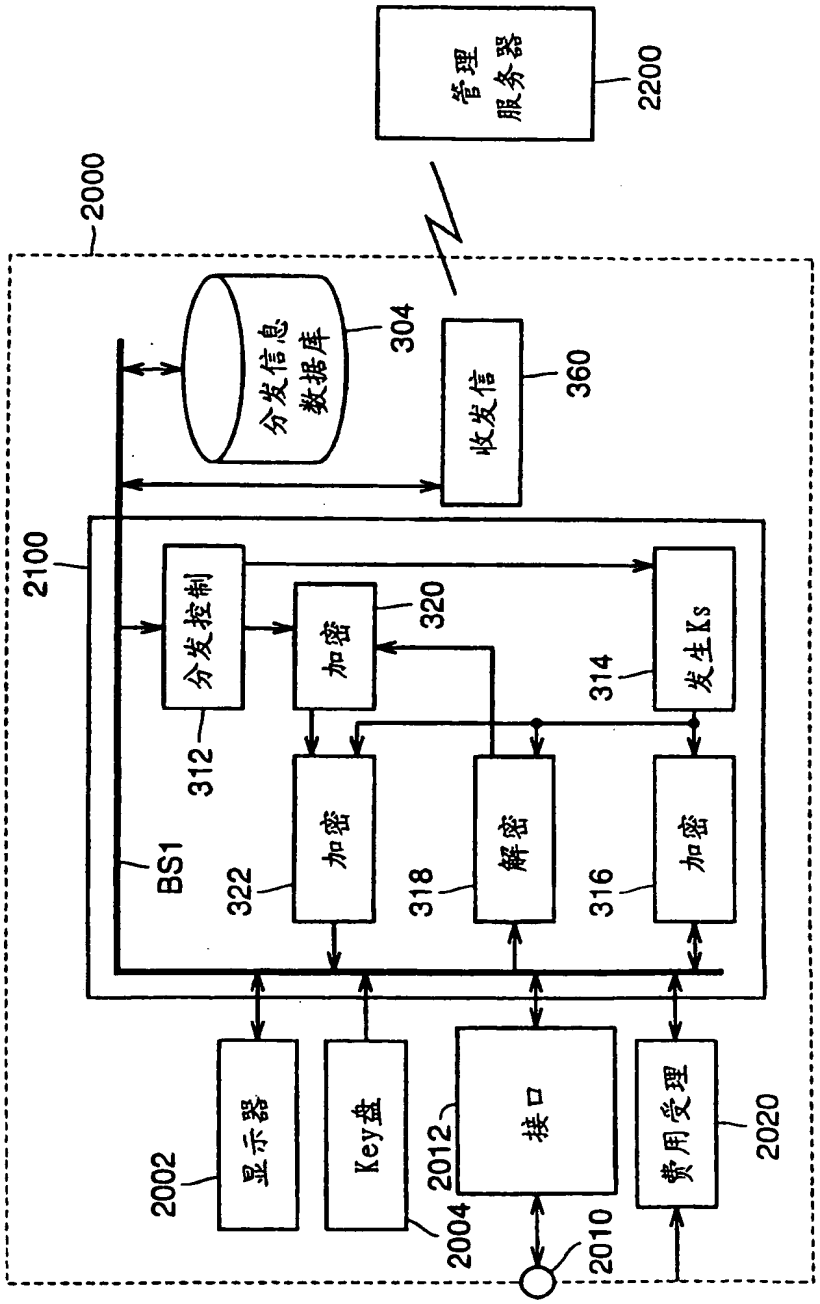

管理服务器
2200
2000
分发信息数据库
304
收发信
360
2100
分发控制
312
加密
320
发生Ks
314
BS1
加密
322
解密
318
加密
316
显示器
2002
Key盘
2004
接口
2012
2010
费用受理
2020

图 21

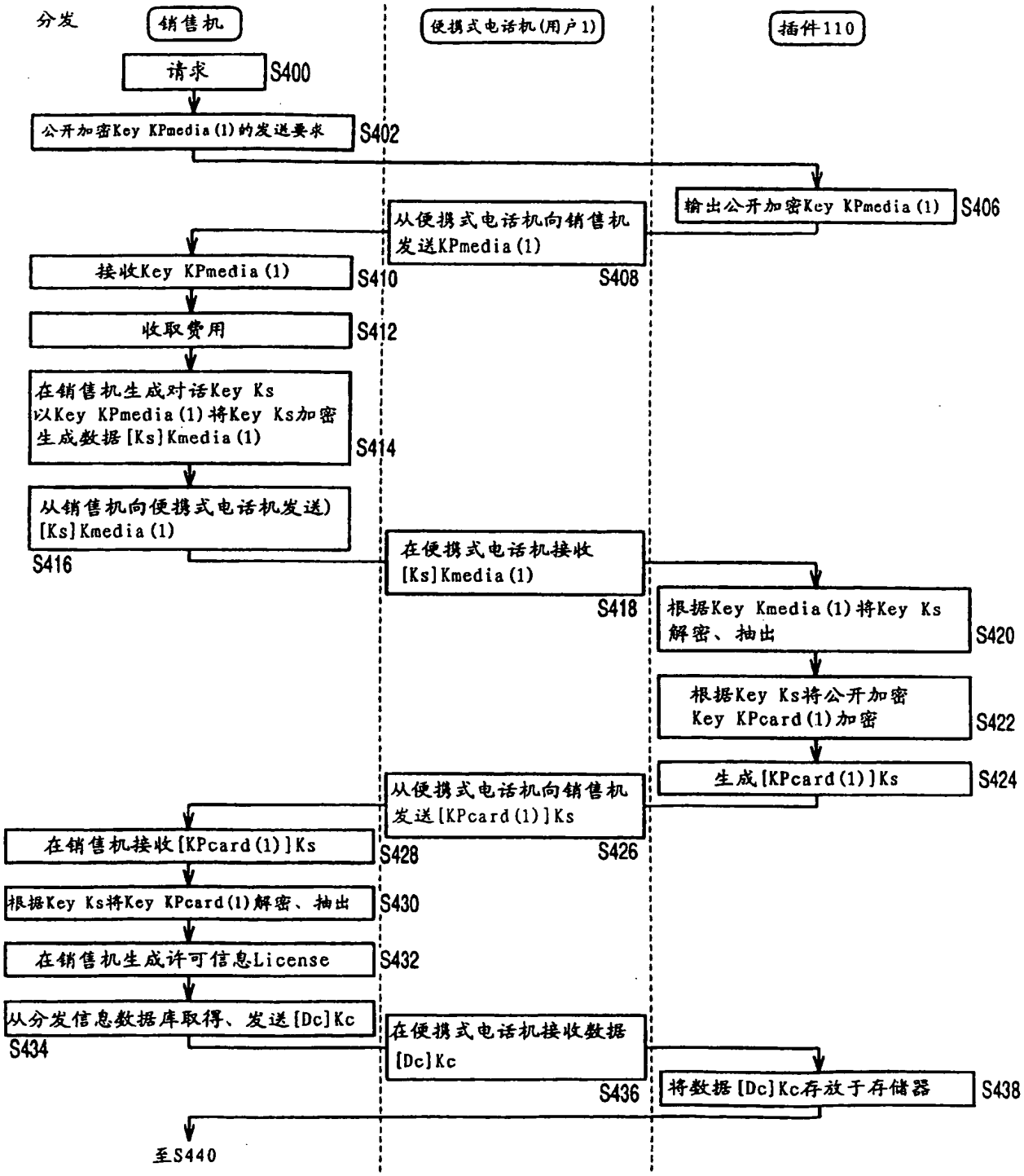

分发
销售机
便携式电话机(用户1)
插件110
请求
S400
公开加密Key KPmedia(1)的发送要求
S402
输出公开加密Key KPmedia(1)
S406
从便携式电话机向销售机发送KPmedia(1)
S408
接收Key KPmedia(1)
S410
收取费用
S412
在销售机生成对话Key Ks以Key KPmedia(1)将Key Ks加密生成数据[Ks]Kmedia(1)
S414
从销售机向便携式电话机发送)[Ks]Kmedia(1)
S416
在便携式电话机接收[Ks]Kmedia(1)
S418
根据Key Kmedia(1)将Key Ks解密、抽出
S420
根据Key Ks将公开加密Key KPcard(1)加密
S422
生成[KPcard(1)]Ks
S424
从便携式电话机向销售机发送[KPcard(1)]Ks
S426
在销售机接收[KPcard(1)]Ks
S428
根据Key Ks将Key KPcard(1)解密、抽出
S430
在销售机生成许可信息License
S432
从分发信息数据库取得、发送[Dc]Kc
S434
在便携式电话机接收数据[Dc]Kc
S436
将数据[Dc]Kc存放于存储器
S438
至S440

图 22

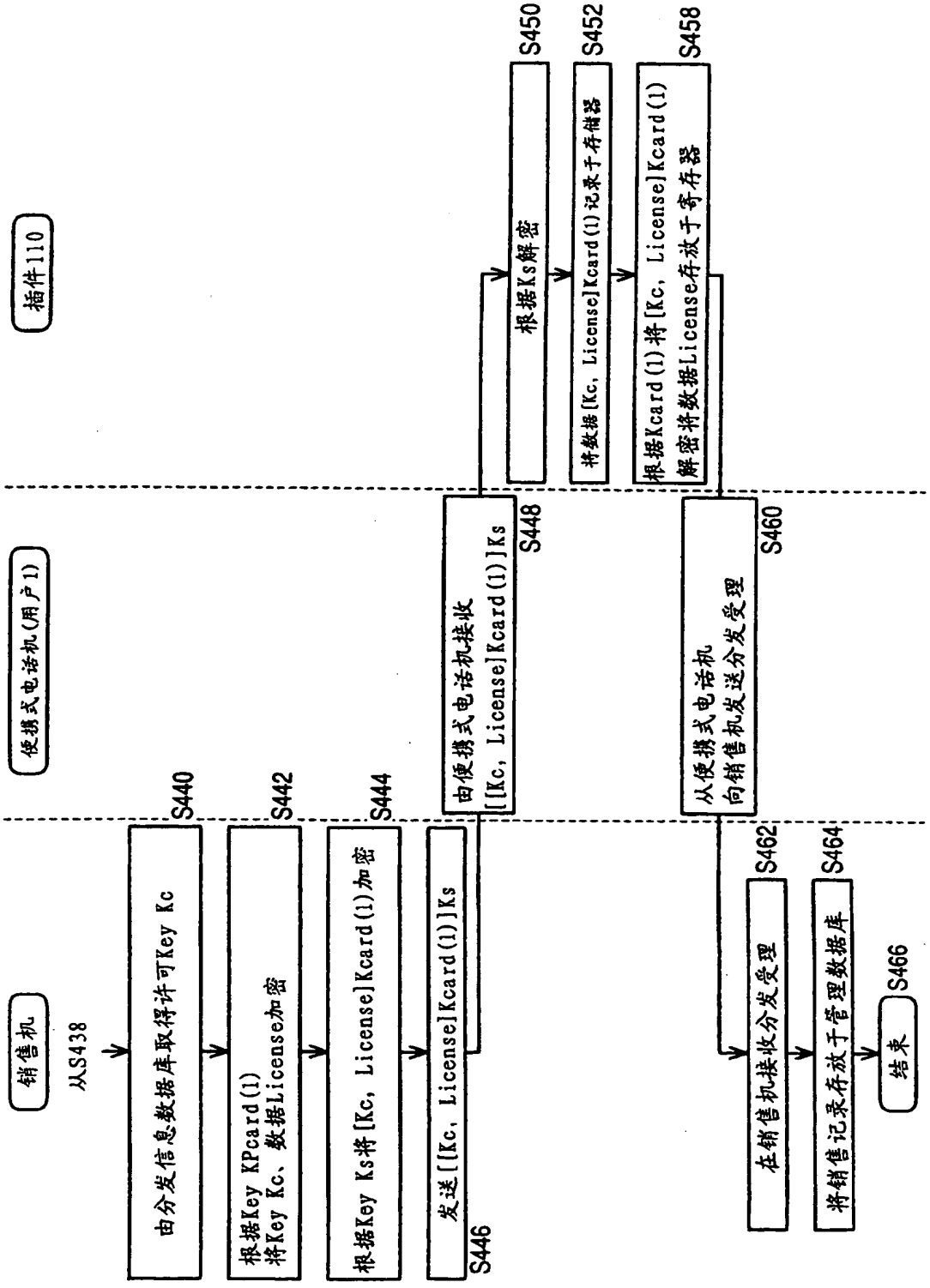

销售机
便携式电话机(用户1)
插件110
从S438
由分发信息数据库取得许可Key Kc
S440
根据Key KPcard(1)
将Key Kc、数据License加密
S442
根据Key Ks将[Kc, License]Kcard(1)加密
S444
发送{[Kc, License]Kcard(1)]Ks
S446
由便携式电话机接收
{[Kc, License]Kcard(1)]Ks
S448
根据Ks解密
S450
将数据[Kc, License]Kcard(1)记录于存储器
S452
根据Kcard(1)将[Kc, License]Kcard(1)
解密将数据License存放于寄存器
S458
从便携式电话机
向销售机发送分发受理
S460
在销售机接收分发受理
S462
将销售记录存放于管理数据库
S464
结束
S466

图 23

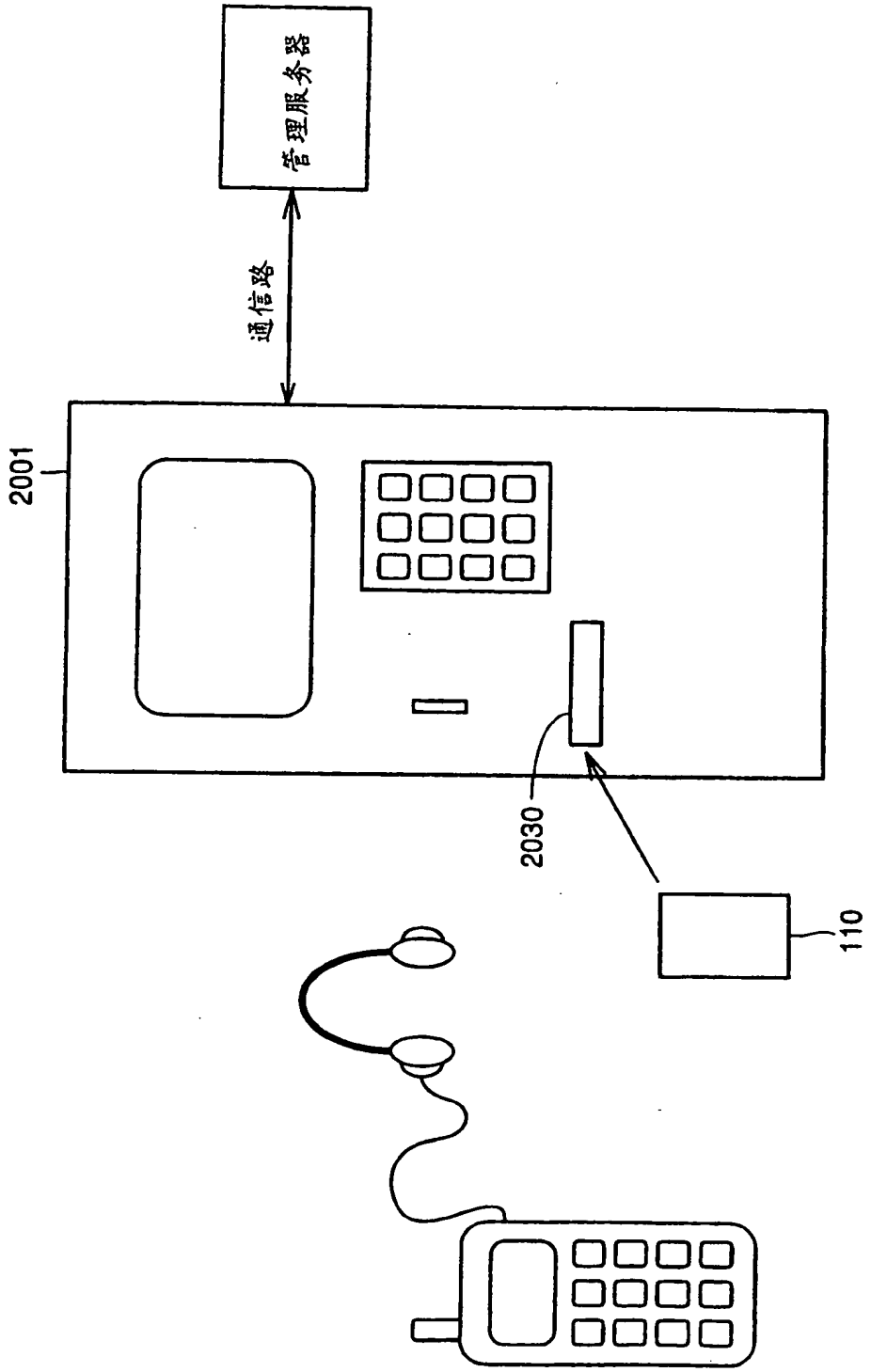


图 24

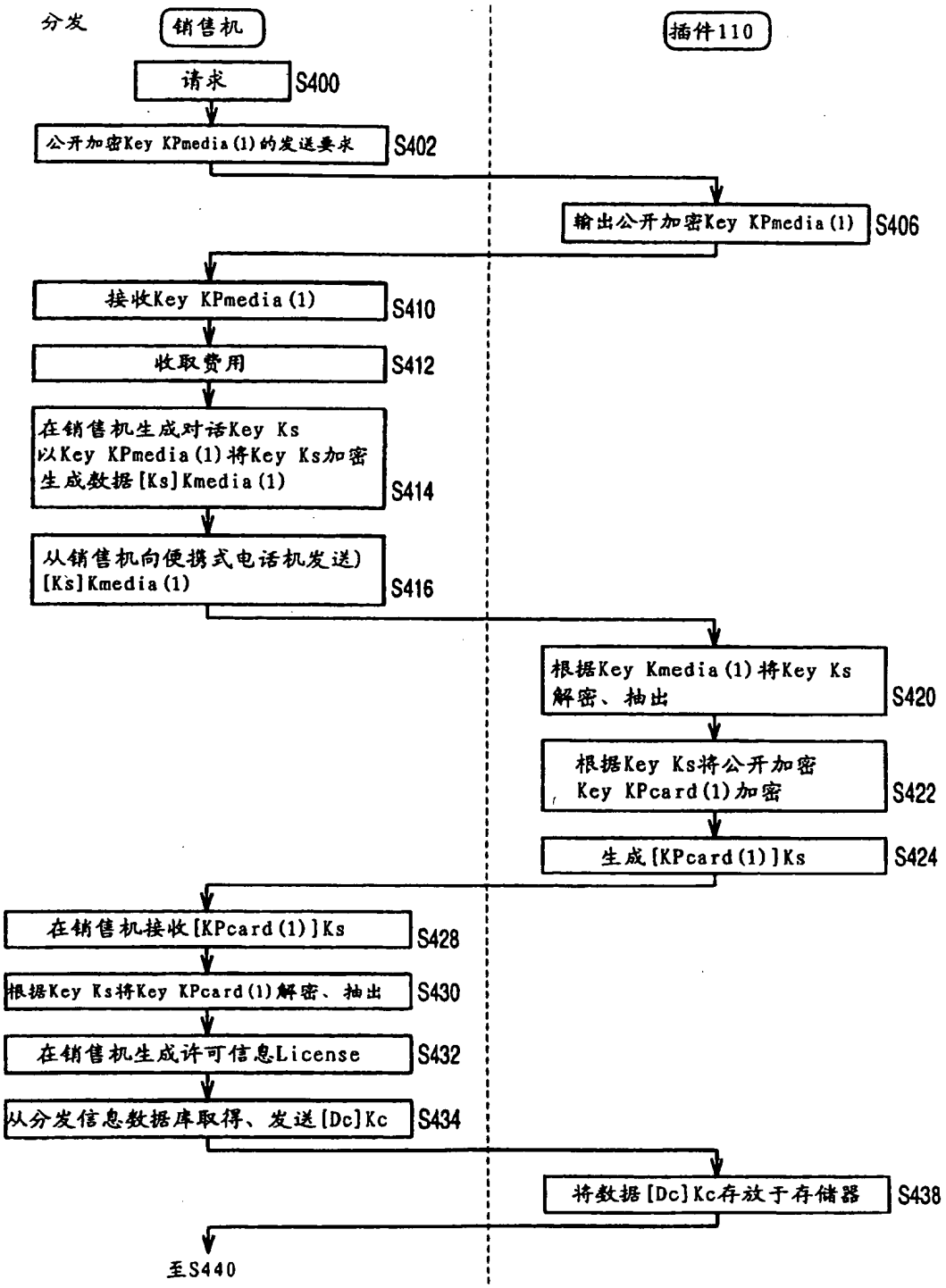

分发
销售机
插件110
请求
S400
公开加密Key KPmedia(1)的发送要求
S402
输出公开加密Key KPmedia(1)
S406
接收Key KPmedia(1)
S410
收取费用
S412
在销售机生成对话Key Ks
以Key KPmedia(1)将Key Ks加密
生成数据[Ks]Kmedia(1)
S414
从销售机向便携式电话机发送)
[Ks]Kmedia(1)
S416
根据Key Kmedia(1)将Key Ks
解密、抽出
S420
根据Key Ks将公开加密
Key KPcard(1)加密
S422
生成[KPcard(1)]Ks
S424
在销售机接收[KPcard(1)]Ks
S428
根据Key Ks将Key KPcard(1)解密、抽出
S430
在销售机生成许可信息License
S432
从分发信息数据库取得、发送[Dc]Kc
S434
将数据[Dc]Kc存放于存储器
S438
至S440

图 25

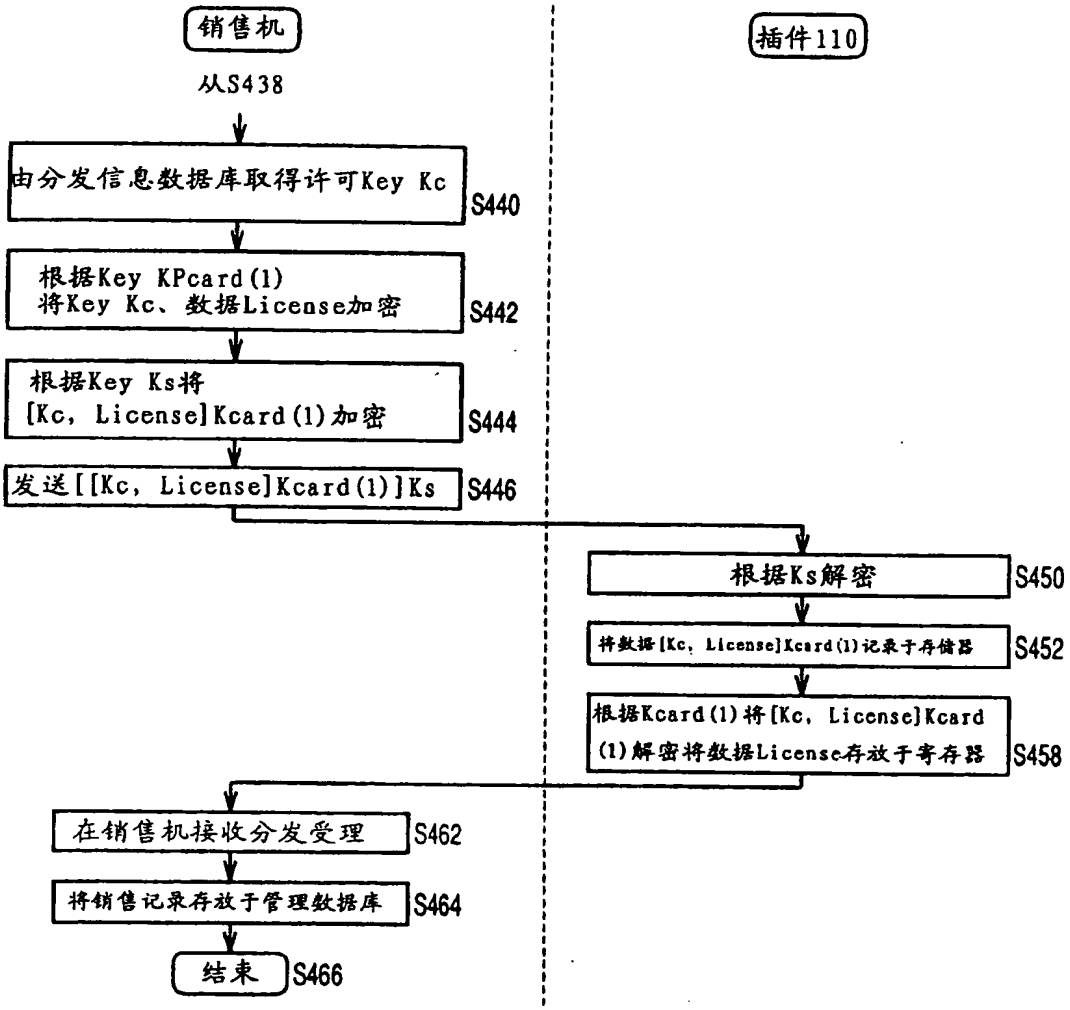

销售机
插件110
从S438
由分发信息数据库取得许可Key Kc
S440
根据Key KPcard(1)
将Key Kc、数据License加密
S442
根据Key Ks将
[Kc, License]Kcard(1)加密
S444
发送[[Kc, License]Kcard(1)]Ks
S446
根据Ks解密
S450
将数据[Kc, License]Kcard(1)记录于存储器
S452
根据Kcard(1)将[Kc, License]Kcard
(1)解密将数据License存放于寄存器
S458
在销售机接收分发受理
S462
将销售记录存放于管理数据库
S464
结束
S466

图 26

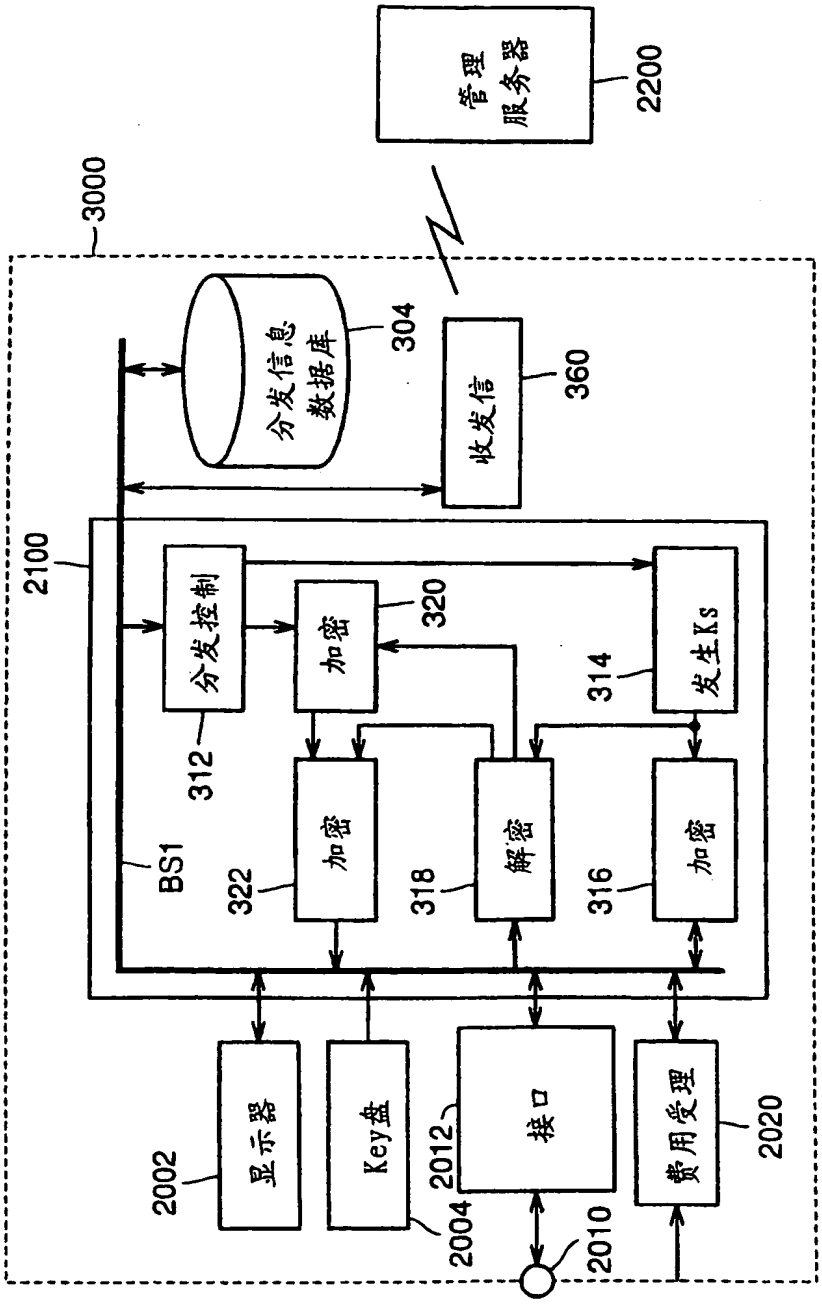

管理服务器
2200
3000
分发信息数据库
304
收发信
360
2100
分发控制
312
加密
320
发生Ks
314
BS1
加密
322
解密
318
加密
316
显示器
2002
Key盘
2004
接口
2012
费用受理
2020
2010

图 27

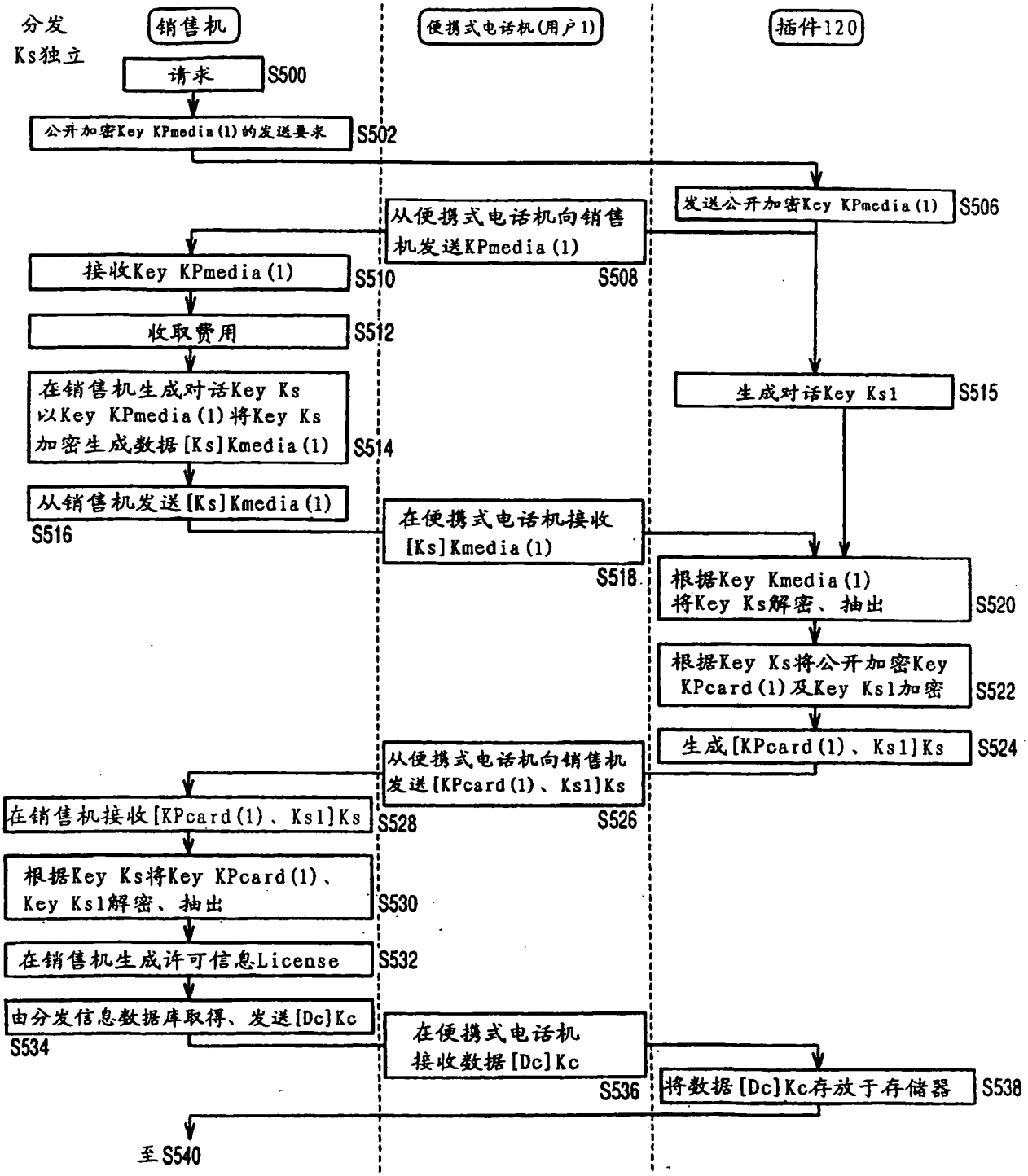

分发
Ks独立
销售机
便携式电话机(用户1)
插件120
请求
S500
公开加密Key KPmedia(1)的发送要求
S502
发送公开加密Key KPmedia(1)
S506
从便携式电话机向销售机发送KPmedia(1)
S508
接收Key KPmedia(1)
S510
收取费用
S512
在销售机生成对话Key Ks以Key KPmedia(1)将Key Ks加密生成数据[Ks]Kmedia(1)
S514
生成对话Key Ks1
S515
从销售机发送[Ks]Kmedia(1)
S516
在便携式电话机接收[Ks]Kmedia(1)
S518
根据Key Kmedia(1)将Key Ks解密、抽出
S520
根据Key Ks将公开加密Key KPcard(1)及Key Ks1加密
S522
生成[KPcard(1)、Ks1]Ks
S524
从便携式电话机向销售机发送[KPcard(1)、Ks1]Ks
S526
在销售机接收[KPcard(1)、Ks1]Ks
S528
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S530
在销售机生成许可信息License
S532
由分发信息数据库取得、发送[Dc]Kc
S534
在便携式电话机接收数据[Dc]Kc
S536
将数据[Dc]Kc存放于存储器
S538
至S540

图 28

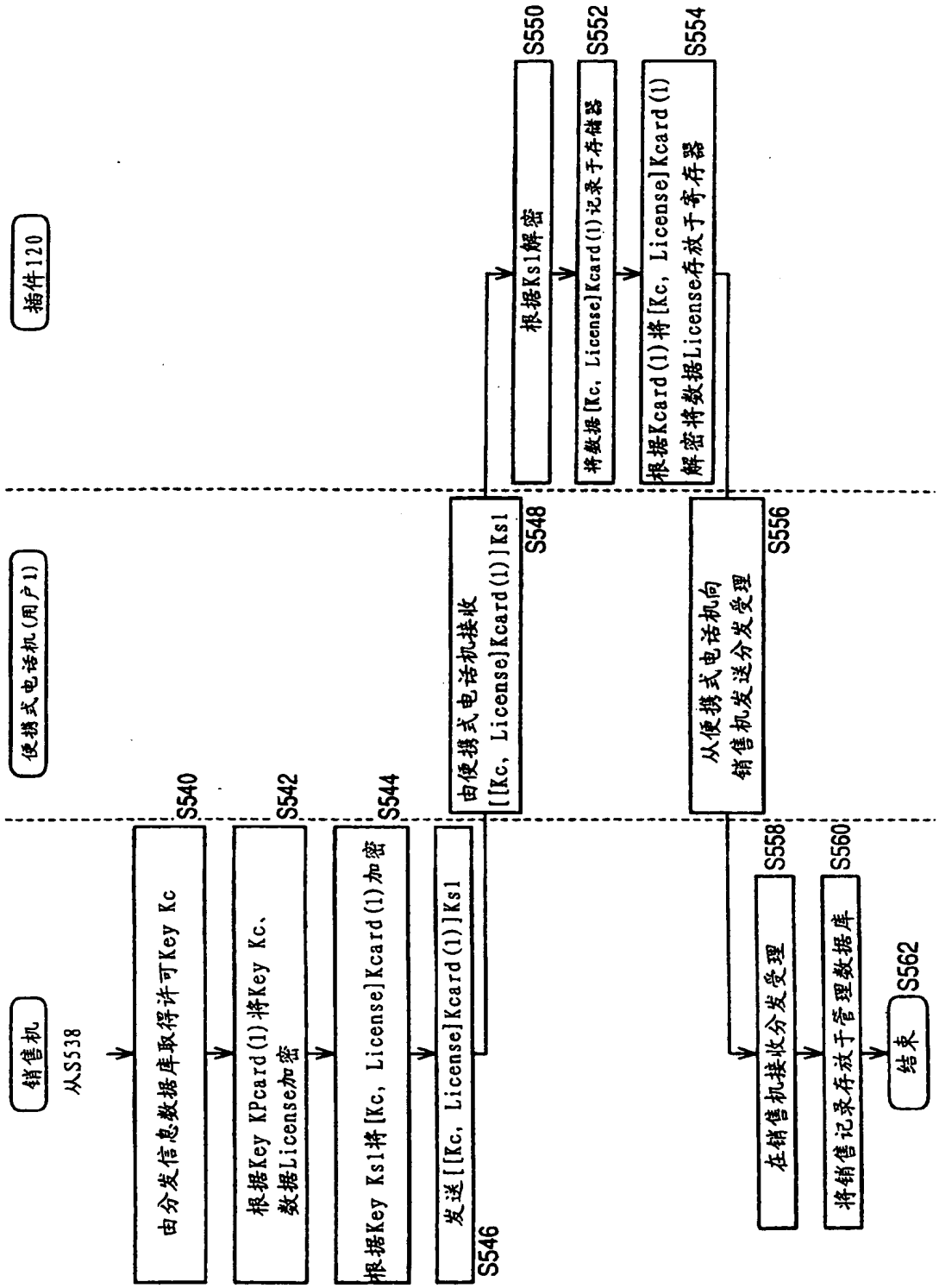

销售机
从S538
便携式电话机(用户1)
插件120
由分发信息数据库取得许可Key Kc
S540
根据Key KPcard(1)将Key Kc、数据License加密
S542
根据Key Ks1将[Kc, License]Kcard(1)加密
S544
发送[[Kc, License]Kcard(1)]Ks1
S546
由便携式电话机接收[[Kc, License]Kcard(1)]Ks1
S548
根据Ks1解密
S550
将数据[Kc, License]Kcard(1)记录于存储器
S552
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S554
从便携式电话机向销售机发送分发受理
S556
在销售机接收分发受理
S558
将销售记录存放于管理数据库
S560
结束
S562

图 29

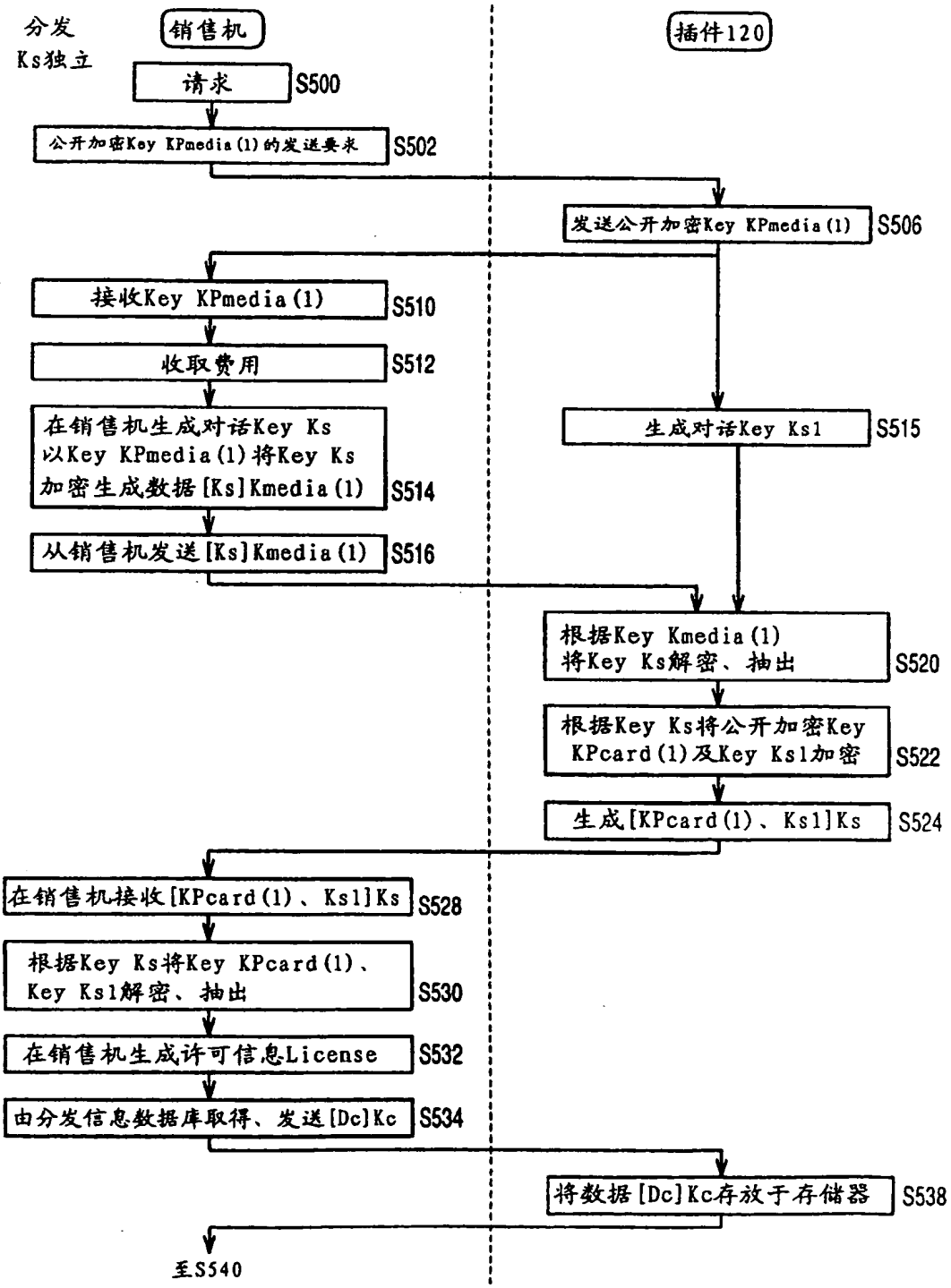

分发
Ks独立
销售机
插件120
请求
S500
公开加密Key KPmedia(1)的发送要求
S502
发送公开加密Key KPmedia(1)
S506
接收Key KPmedia(1)
S510
收取费用
S512
在销售机生成对话Key Ks
以Key KPmedia(1)将Key Ks
加密生成数据[Ks]Kmedia(1)
S514
生成对话Key Ks1
S515
从销售机发送[Ks]Kmedia(1)
S516
根据Key Kmedia(1)
将Key Ks解密、抽出
S520
根据Key Ks将公开加密Key
KPcard(1)及Key Ks1加密
S522
生成[KPcard(1)、Ks1]Ks
S524
在销售机接收[KPcard(1)、Ks1]Ks
S528
根据Key Ks将Key KPcard(1)、
Key Ks1解密、抽出
S530
在销售机生成许可信息License
S532
由分发信息数据库取得、发送[Dc]Kc
S534
将数据[Dc]Kc存放于存储器
S538
至S540

图 30

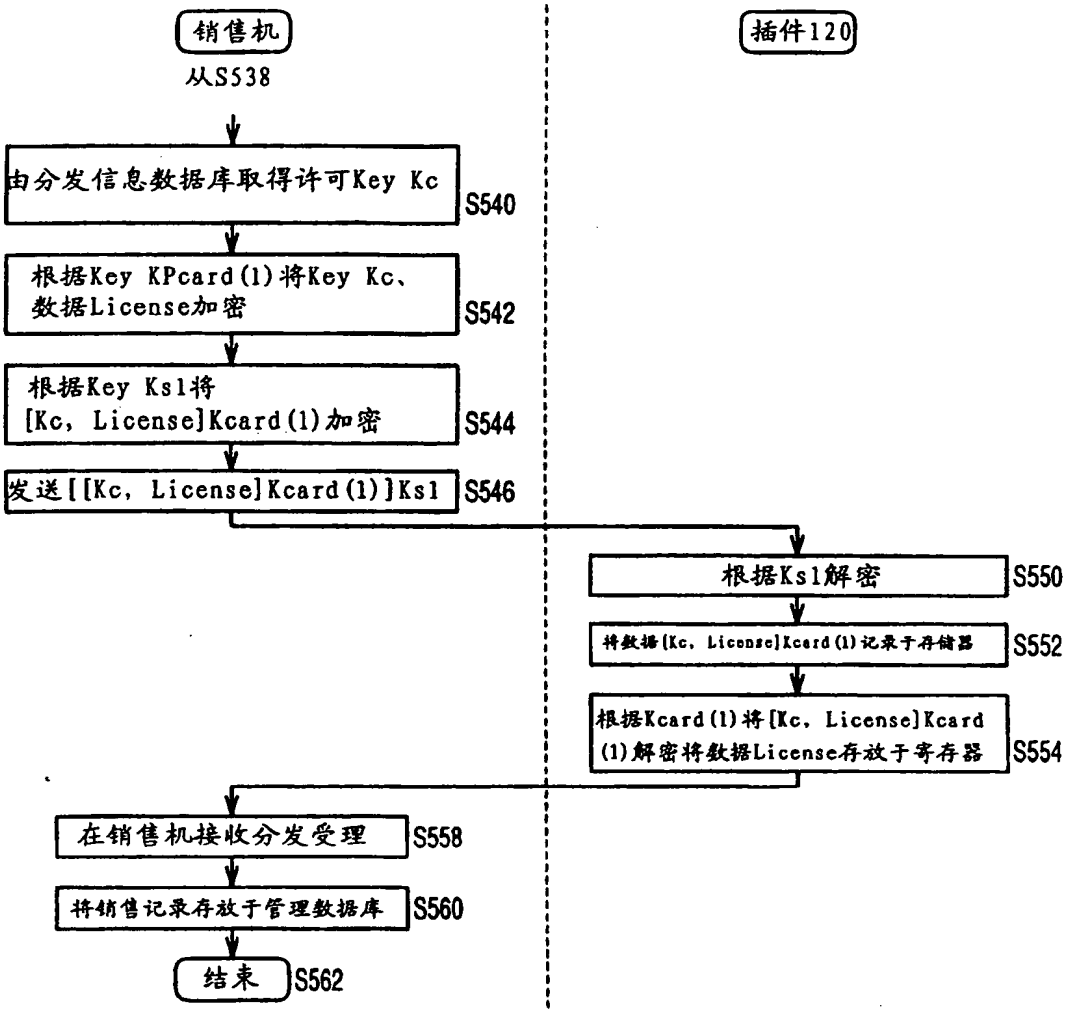

销售机
插件120
从S538
由分发信息数据库取得许可Key Kc
S540
根据Key KPcard(1)将Key Kc、数据License加密
S542
根据Key Ks1将[Kc, License]Kcard(1)加密
S544
发送[[Kc, License]Kcard(1)]Ks1
S546
根据Ks1解密
S550
将数据[Kc, License]Kcard(1)记录于存储器
S552
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S554
在销售机接收分发受理
S558
将销售记录存放于管理数据库
S560
结束
S562

图 31

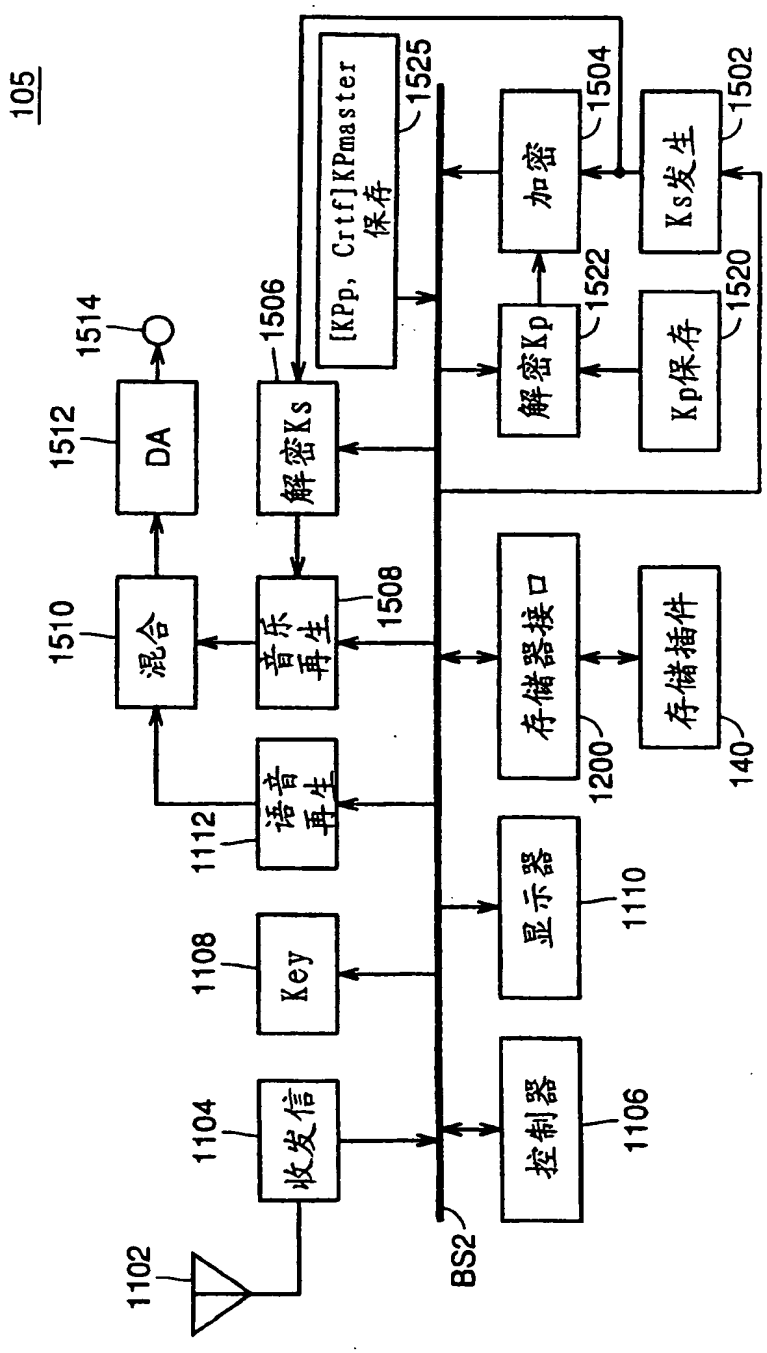

105
1102
1104
收发信
1108
Key
1112
语音再生
1510
混合
1512
DA
1514
1506
解密Ks
1508
音乐再生
BS2
控制器
1106
显示器
1110
存储器接口
1200
存储插件
140
[KPp, Crtf]KPmaster保存
1525
解密Kp
1522
Kp保存
1520
加密
1504
Ks发生
1502

图 32

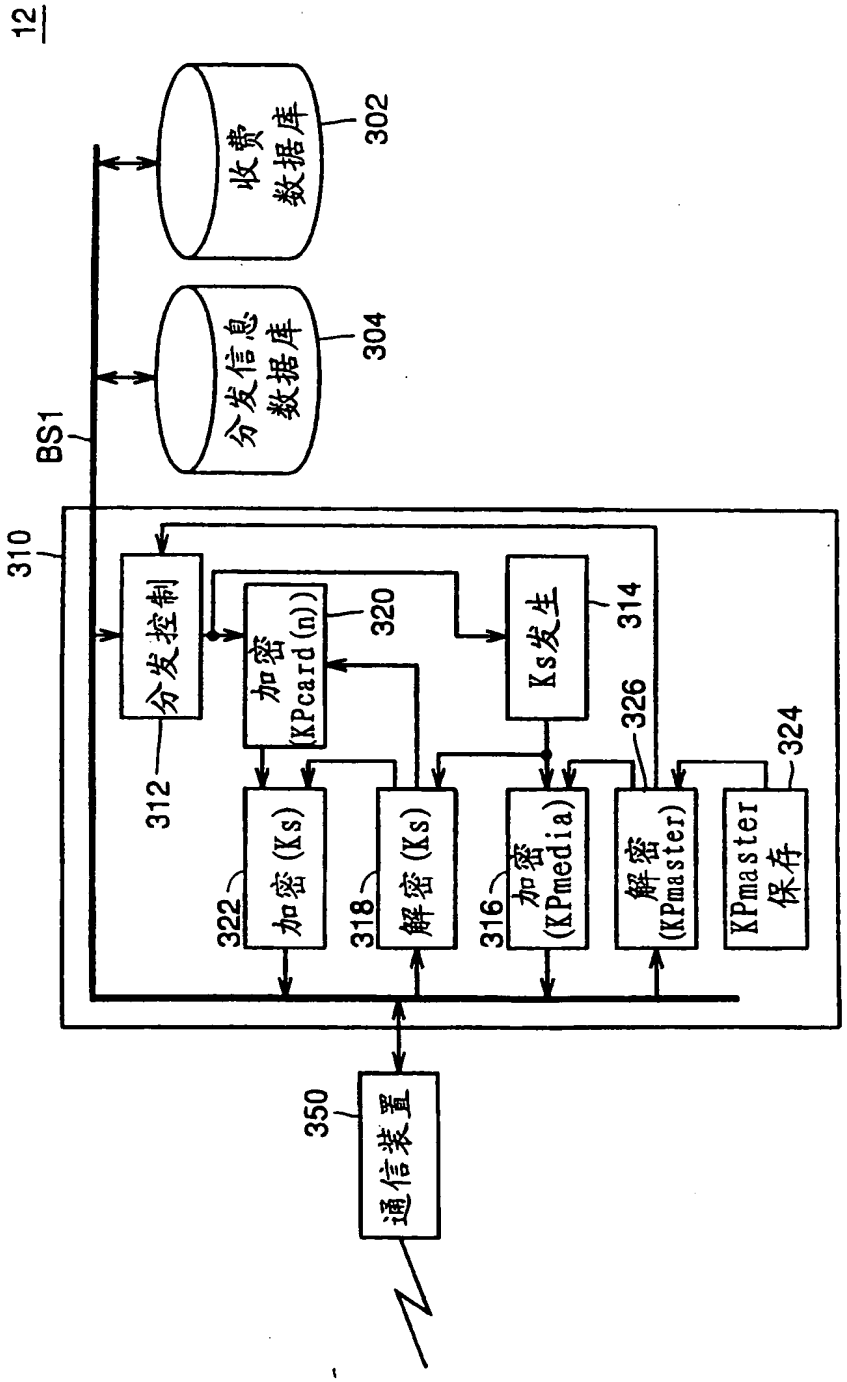

12
收费数据库
302
分发信息数据库
304
BS1
310
分发控制
312
加密(KPcard(n))
320
Ks发生
314
加密(Ks)
322
解密(Ks)
318
加密(KPmedia)
316
解密(KPmaster)
326
KPmaster保存
324
通信装置
350

图 33

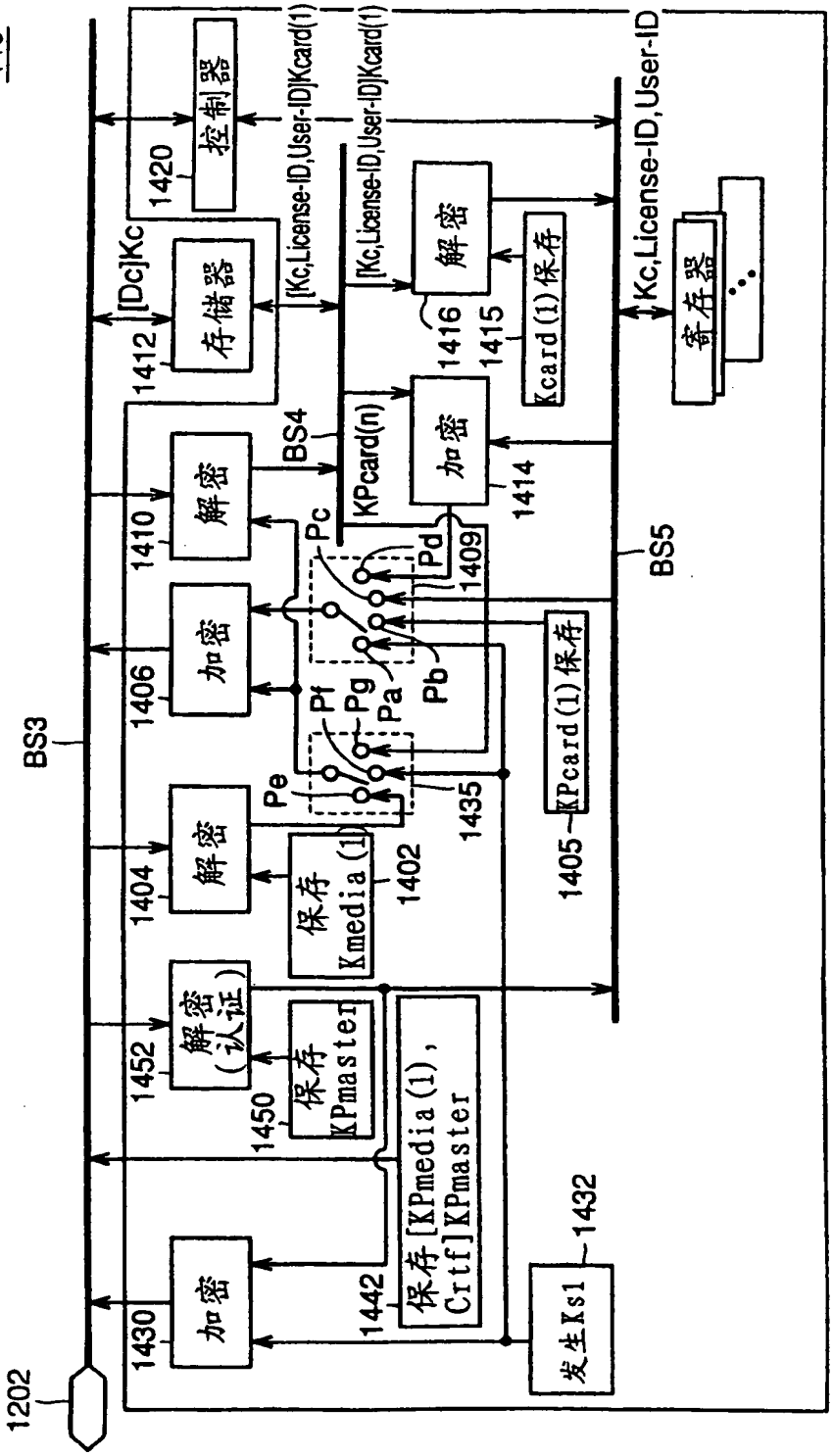

140
1202
BS3
BS4
BS5
1430
加密
1442
保存[KPmedia(1),Crtf]KPmaster
1432
发生Ks1
1452
解密(认证)
1450
保存KPmaster
1404
解密
1402
保存Kmedia(1)
1406
加密
1410
解密
1412
存储器
1420
控制器
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
Pe
Pf
Pg
Pa
Pb
Pc
Pd
1435
1405
KPcard(1)保存
KPcard(n)
1409
1414
加密
1415
Kcard(1)保存
1416
解密
Kc,License-ID,User-ID
存储器

图 34

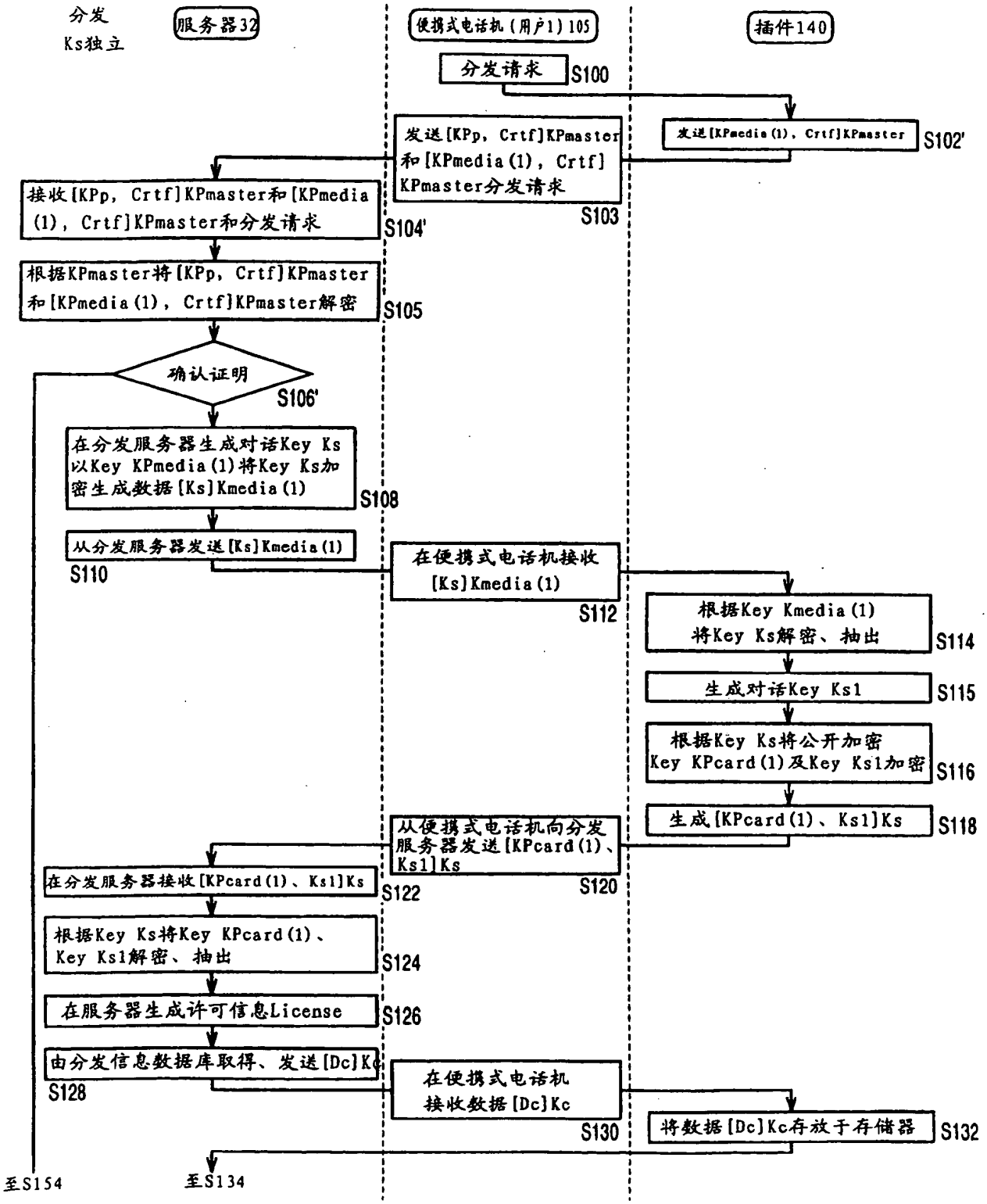

分发
Ks独立
服务器32
便携式电话机（用户1）105
插件140
分发请求
S100
发送[KPp，Crtf]KPmaster和[KPmedia(1)，Crtf]KPmaster分发请求
S103
发送[KPmedia(1)，Crtf]KPmaster
S102'
接收[KPp，Crtf]KPmaster和[KPmedia(1)，Crtf]KPmaster和分发请求
S104'
根据KPmaster将[KPp，Crtf]KPmaster和[KPmedia(1)，Crtf]KPmaster解密
S105
确认证明
S106'
在分发服务器生成对话Key Ks以Key KPmedia(1)将Key Ks加密生成数据[Ks]Kmedia(1)
S108
从分发服务器发送[Ks]Kmedia(1)
S110
在便携式电话机接收[Ks]Kmedia(1)
S112
根据Key Kmedia(1)将Key Ks解密、抽出
S114
生成对话Key Ks1
S115
根据Key Ks将公开加密Key KPcard(1)及Key Ks1加密
S116
生成[KPcard(1)、Ks1]Ks
S118
从便携式电话机向分发服务器发送[KPcard(1)、Ks1]Ks
S120
在分发服务器接收[KPcard(1)、Ks1]Ks
S122
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S124
在服务器生成许可信息License
S126
由分发信息数据库取得、发送[Dc]Kc
S128
在便携式电话机接收数据[Dc]Kc
S130
将数据[Dc]Kc存放于存储器
S132
至S154
至S134

图 35

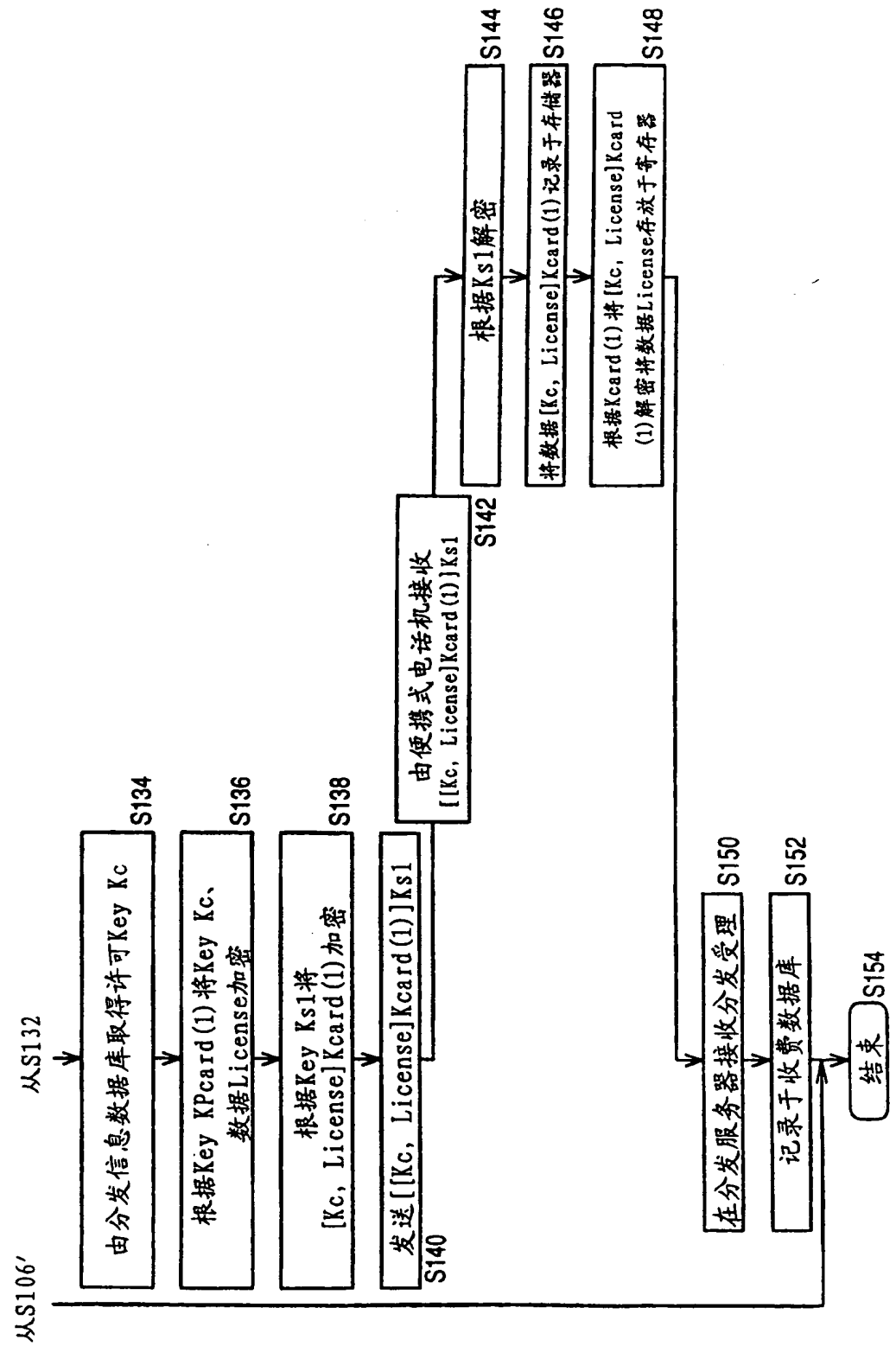

从S106'
从S132
由分发信息数据库取得许可Key Kc
S134
根据Key KPcard(1)将Key Kc、数据License加密
S136
根据Key Ks1将[Kc, License]Kcard(1)加密
S138
发送[[Kc, License]Kcard(1)]Ks1
S140
由便携式电话机接收[[Kc, License]Kcard(1)]Ks1
S142
根据Ks1解密
S144
将数据[Kc, License]Kcard(1)记录于存储器
S146
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S148
在分发服务器接收分发受理
S150
记录于收费数据库
S152
结束
S154

图 36

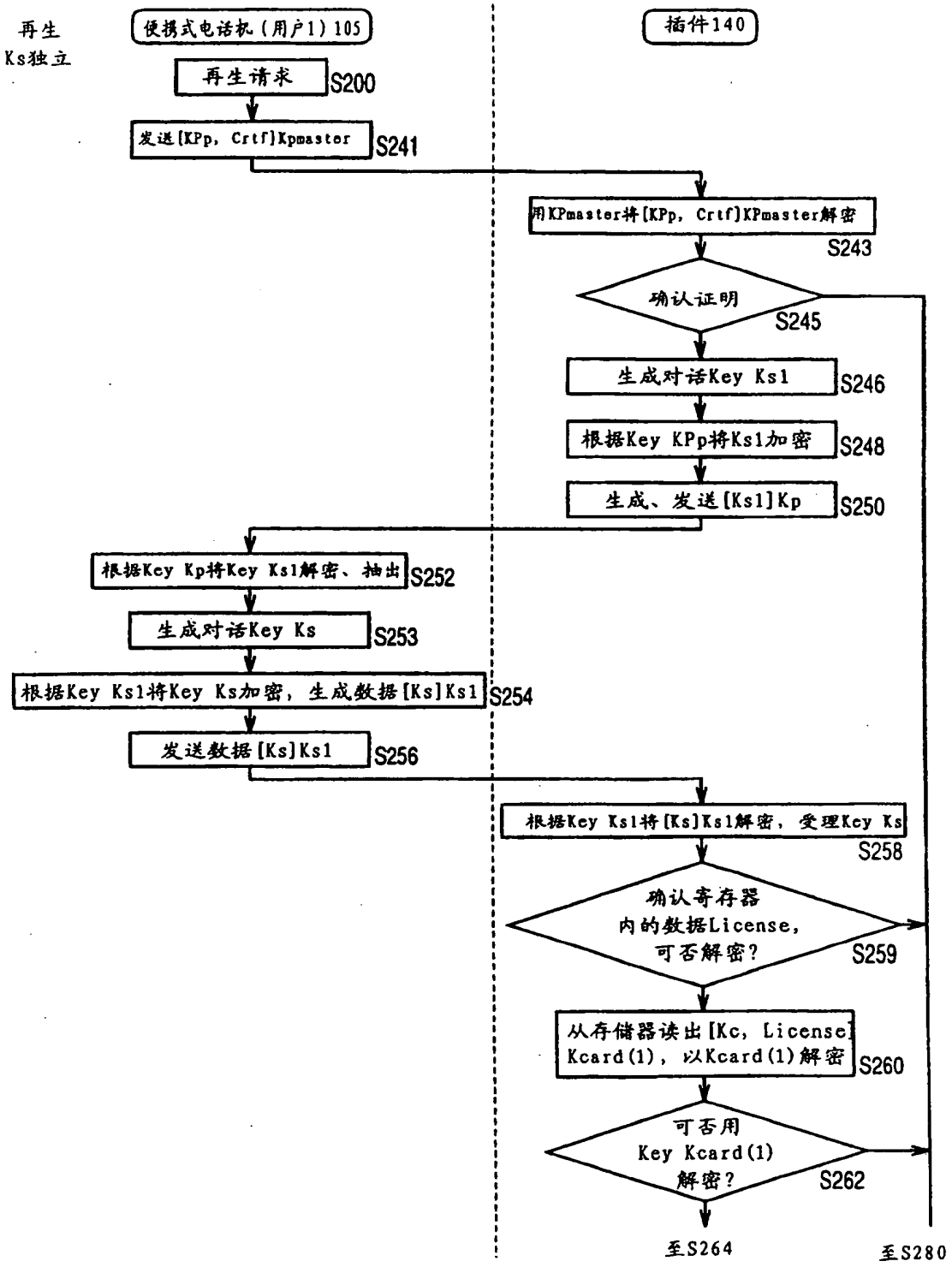

再生
Ks独立
便携式电话机（用户1）105
插件140
再生请求
S200
发送[KPp，Crtf]Kpmaster
S241
用KPmaster将[KPp，Crtf]KPmaster解密
S243
确认证明
S245
生成对话Key Ks1
S246
根据Key KPp将Ks1加密
S248
生成、发送[Ks1]Kp
S250
根据Key Kp将Key Ks1解密、抽出
S252
生成对话Key Ks
S253
根据Key Ks1将Key Ks加密，生成数据[Ks]Ks1
S254
发送数据[Ks]Ks1
S256
根据Key Ks1将[Ks]Ks1解密，受理Key Ks
S258
确认寄存器
内的数据License，
可否解密？
S259
从存储器读出[Kc，License]
Kcard(1)，以Kcard(1)解密
S260
可否用
Key Kcard(1)
解密？
S262
至S264
至S280

图 37

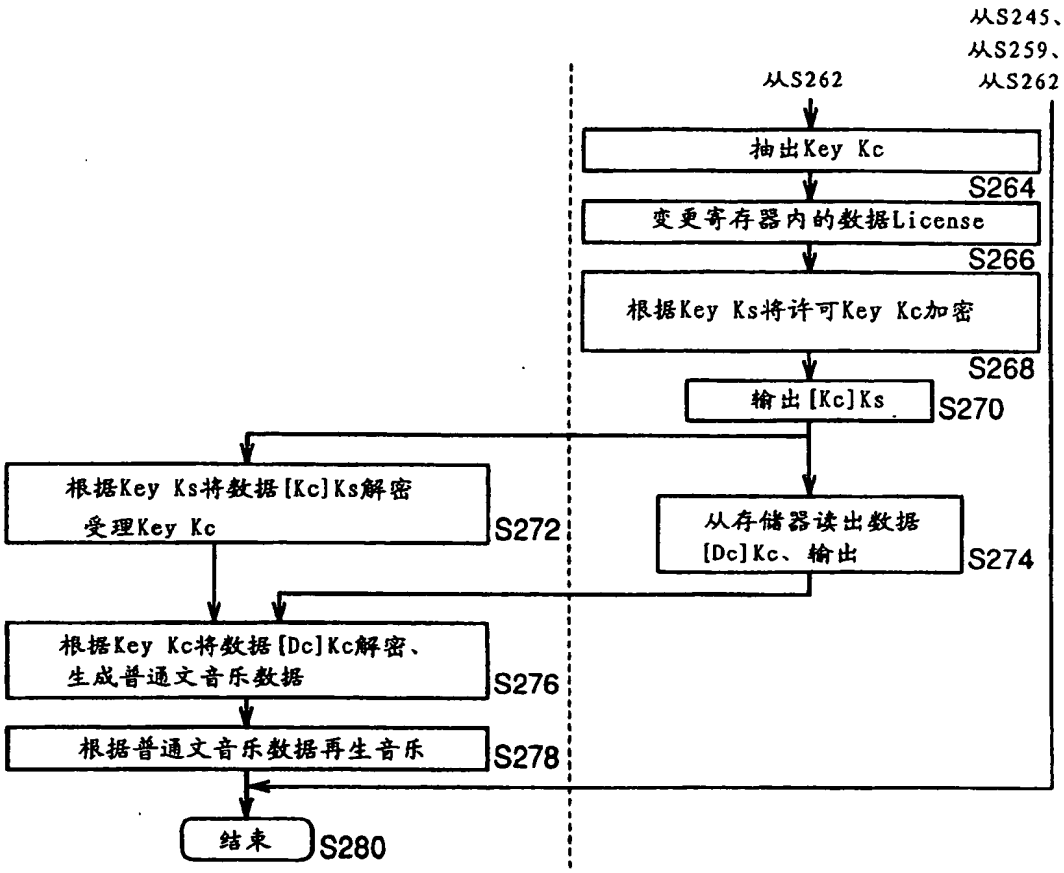

从S245、
从S259、
从S262
从S262
抽出Key Kc
S264
变更寄存器内的数据License
S266
根据Key Ks将许可Key Kc加密
S268
输出[Kc]Ks
S270
根据Key Ks将数据[Kc]Ks解密
受理Key Kc
S272
从存储器读出数据
[Dc]Kc、输出
S274
根据Key Kc将数据[Dc]Kc解密、
生成普通文音乐数据
S276
根据普通文音乐数据再生音乐
S278
结束
S280

图 38

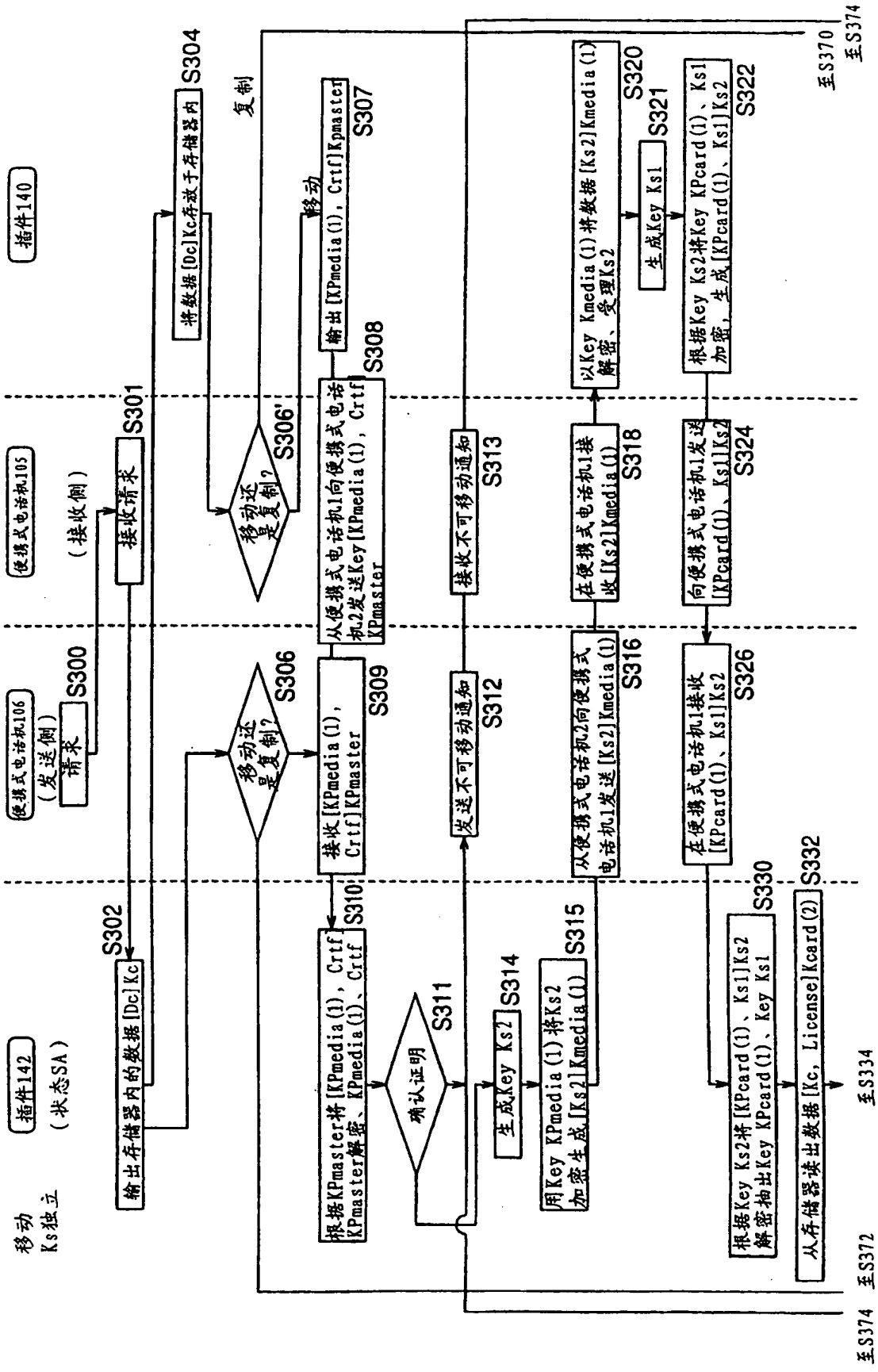

移动
Ks独立
插件142
（状态SA）
便携式电话机106
（发送侧）
请求
S300
输出存储器内的数据[Dc]Kc
S302
便携式电话机105
（接收侧）
接收请求
S301
将数据[Dc]Kc存放于存储器内
S304
插件140
复制
移动还是复制?
S306'
移动
输出[KPmedia(1)，Crtf]Kpmaster
S307
从便携式电话机1向便携式电话机2发送Key[KPmedia(1)，Crtf]KPmaster
S308
移动还是复制?
S306
接收[KPmedia(1)，Crtf]KPmaster
S309
根据KPmaster将[KPmedia(1)，Crtf]KPmaster解密、KPmedia(1)、Crtf
S310
确认证明
S311
发送不可移动通知
S312
接收不可移动通知
S313
生成Key Ks2
S314
用Key KPmedia(1)将Ks2加密生成[Ks2]Kmedia(1)
S315
从便携式电话机2向便携式电话机1发送[Ks2]Kmedia(1)
S316
在便携式电话机1接收[Ks2]Kmedia(1)
S318
以Key Kmedia(1)将数据[Ks2]Kmedia(1)解密、受理Ks2
S320
生成Key Ks1
S321
根据Key Ks2将Key KPcard(1)、Ks1加密，生成[KPcard(1)、Ks1]Ks2
S322
向便携式电话机1发送[KPcard(1)、Ks1]Ks2
S324
在便携式电话机1接收[KPcard(1)、Ks1]Ks2
S326
根据Key Ks2将[KPcard(1)、Ks1]Ks2解密抽出Key KPcard(1)、Key Ks1
S330
从存储器读出数据[Kc，License]Kcard(2)
S332
至S370
至S374
至S372
至S334
至S374

图 39

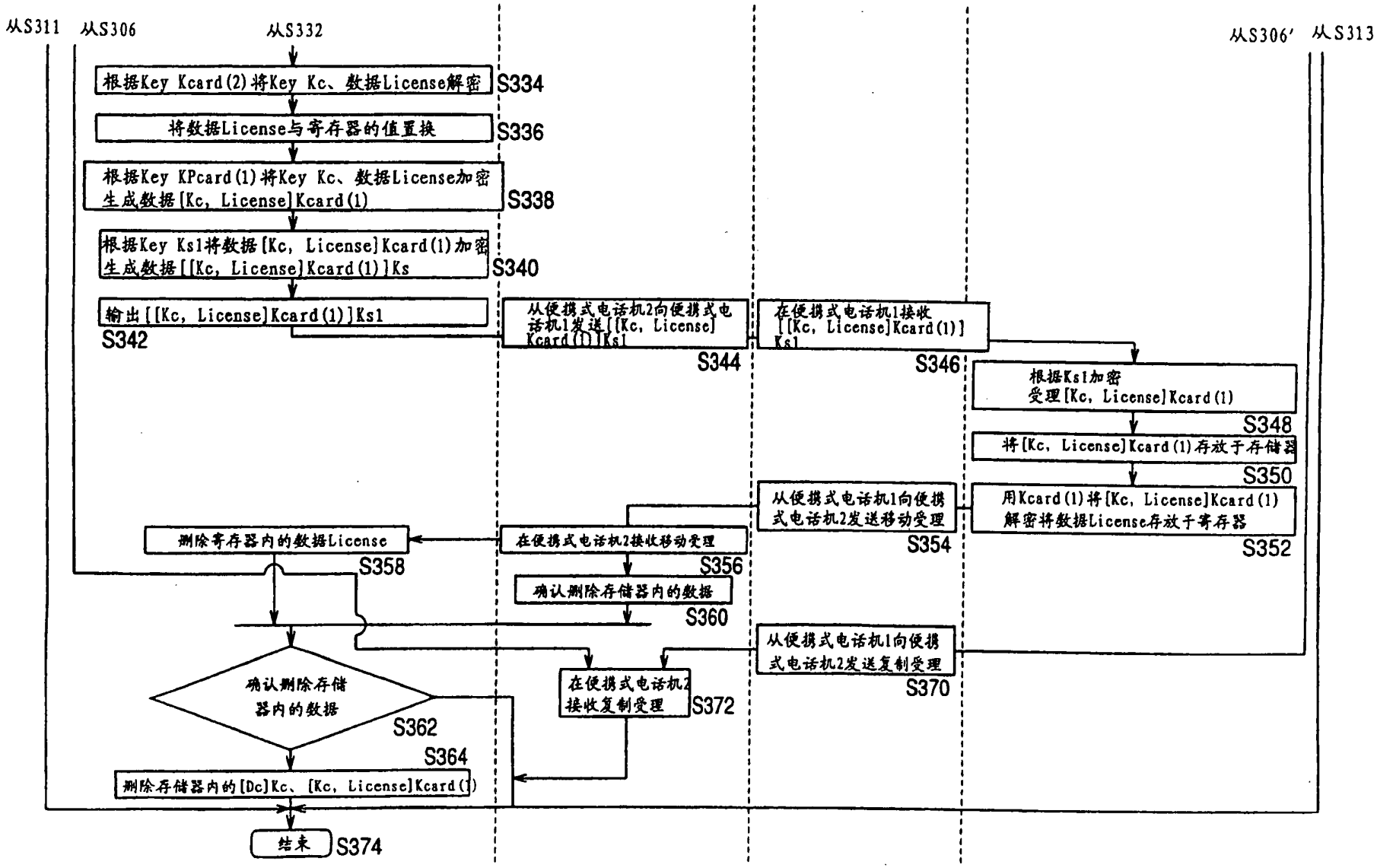

从S311
从S306
从S332
从S306'
从S313
根据Key Kcard(2)将Key Kc、数据License解密
S334
将数据License与寄存器的值置换
S336
根据Key KPcard(1)将Key Kc、数据License加密
生成数据[Kc, License]Kcard(1)
S338
根据Key Ks1将数据[Kc, License]Kcard(1)加密
生成数据[[Kc, License]Kcard(1)]Ks
S340
输出[[Kc, License]Kcard(1)]Ks1
S342
从便携式电话机2向便携式电话机1发送[[Kc, License]Kcard(1)]Ks1
S344
在便携式电话机1接收[[Kc, License]Kcard(1)]Ks1
S346
根据Ks1加密
受理[Kc, License]Kcard(1)
S348
将[Kc, License]Kcard(1)存放于存储器
S350
用Kcard(1)将[Kc, License]Kcard(1)
解密将数据License存放于寄存器
S352
从便携式电话机1向便携式电话机2发送移动受理
S354
在便携式电话机2接收移动受理
S356
删除寄存器内的数据License
S358
确认删除存储器内的数据
S360
从便携式电话机1向便携式电话机2发送复制受理
S370
确认删除存储器内的数据
S362
在便携式电话机2接收复制受理
S372
S364
删除存储器内的[Dc]Kc、[Kc, License]Kcard(1)
结束
S374

图 40

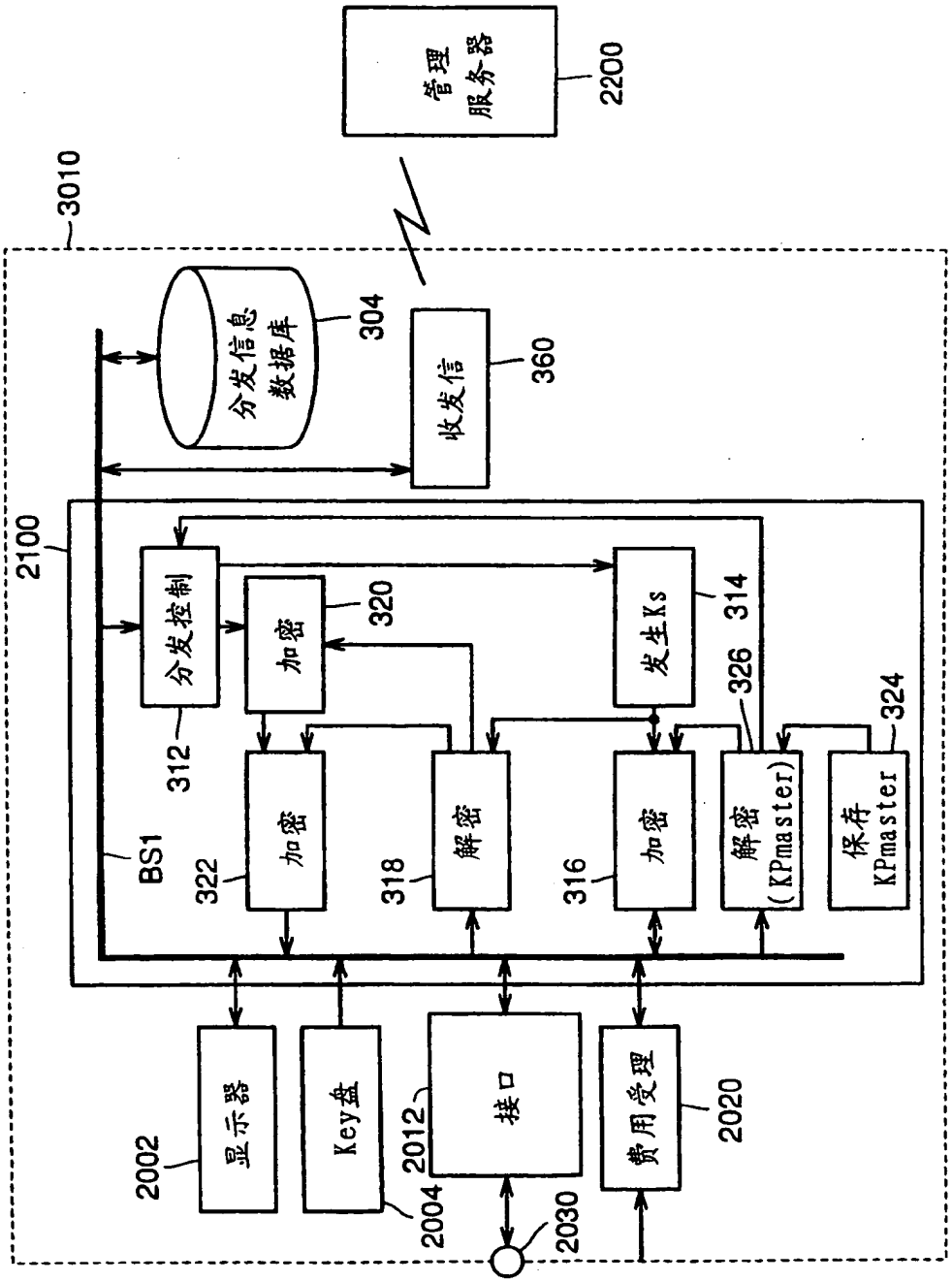

管理服务器
2200
3010
分发信息数据库
304
收发信
360
2100
分发控制
312
加密
320
发生Ks
314
326
324
BS1
322
加密
318
解密
316
加密
解密(KPmaster)
保存KPmaster
显示器
2002
Key盘
2004
2012
接口
2030
费用受理
2020

图 41

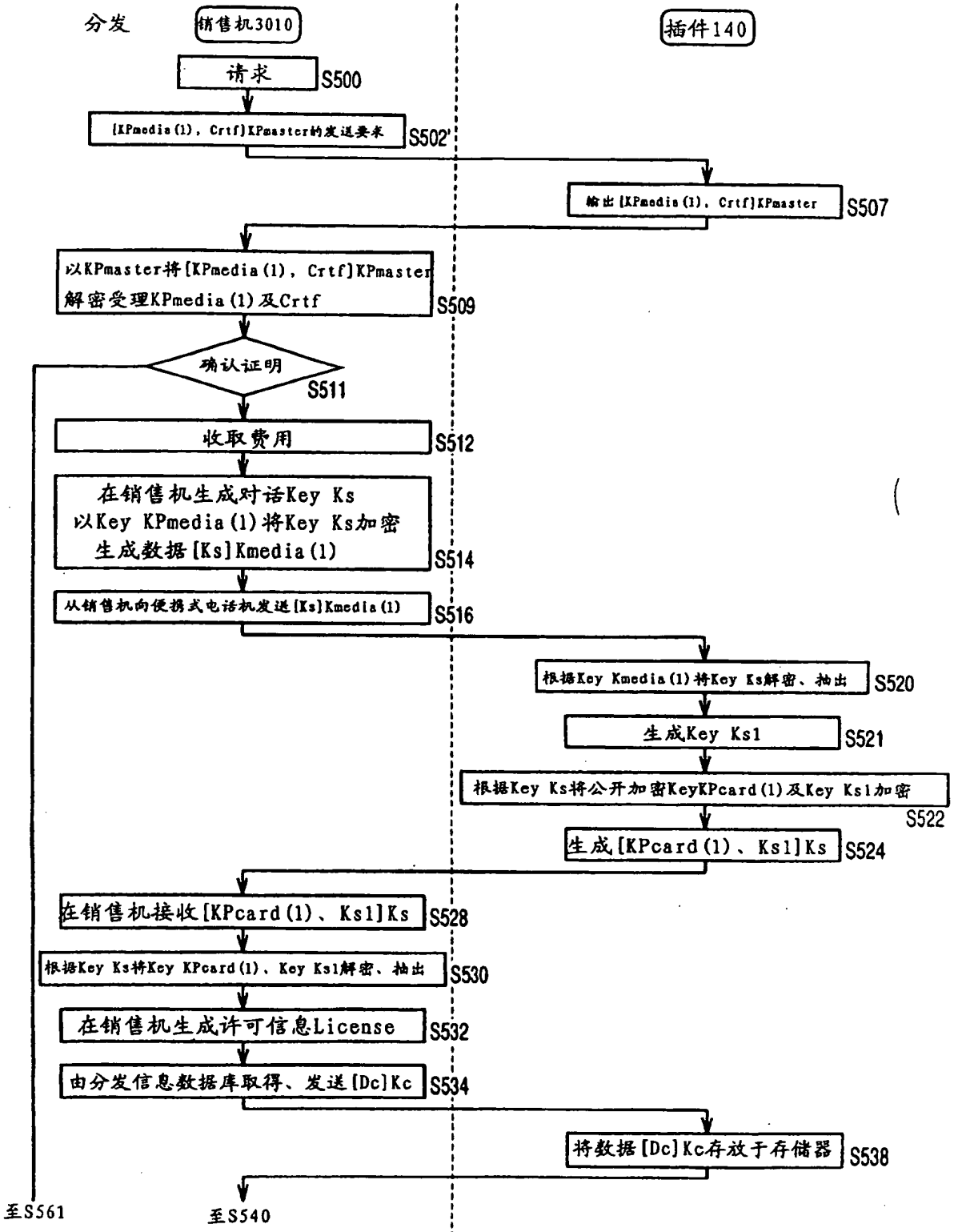

分发
销售机3010
插件140
请求
S500
[KPmedia(1), Crtf]KPmaster的发送要求
S502
输出[KPmedia(1), Crtf]KPmaster
S507
以KPmaster将[KPmedia(1), Crtf]KPmaster
解密受理KPmedia(1)及Crtf
S509
确认证明
S511
收取费用
S512
在销售机生成对话Key Ks
以Key KPmedia(1)将Key Ks加密
生成数据[Ks]Kmedia(1)
S514
从销售机向便携式电话机发送[Ks]Kmedia(1)
S516
根据Key Kmedia(1)将Key Ks解密、抽出
S520
生成Key Ks1
S521
根据Key Ks将公开加密KeyKPcard(1)及Key Ks1加密
S522
生成[KPcard(1)、Ks1]Ks
S524
在销售机接收[KPcard(1)、Ks1]Ks
S528
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S530
在销售机生成许可信息License
S532
由分发信息数据库取得、发送[Dc]Kc
S534
将数据[Dc]Kc存放于存储器
S538
至S561
至S540

图 42

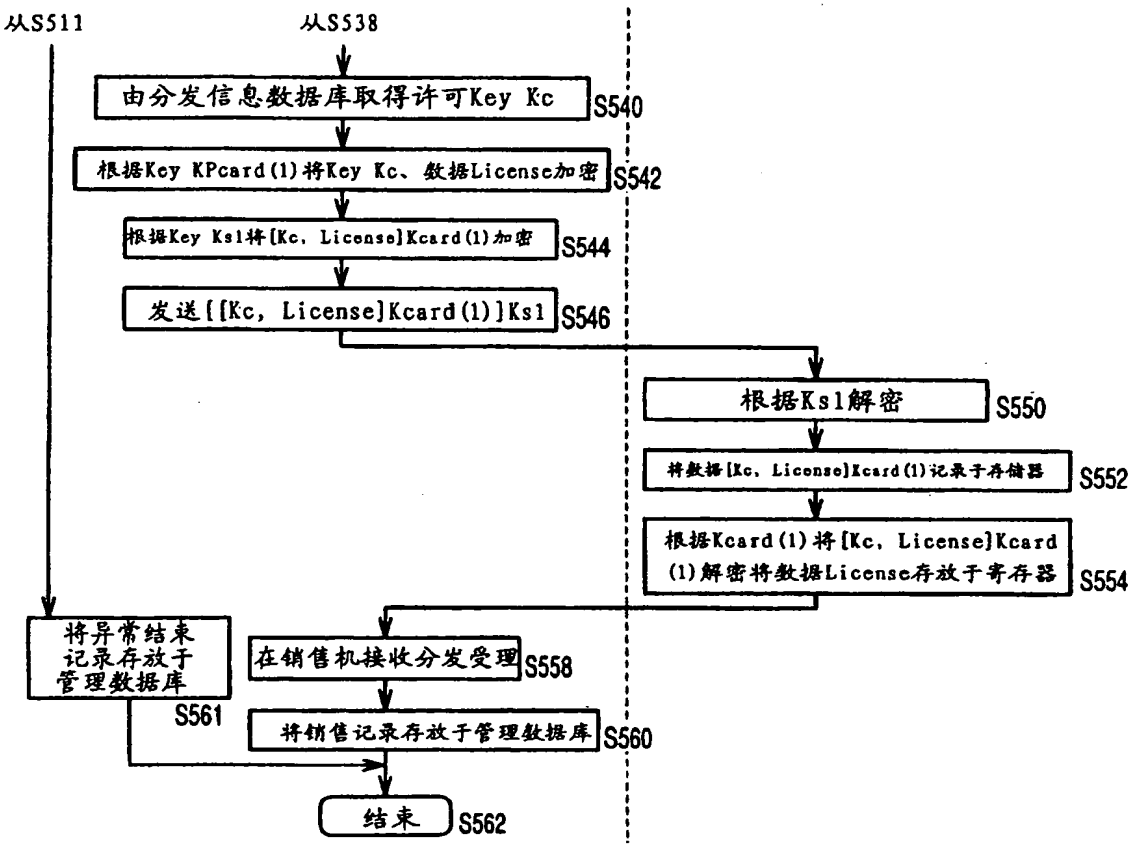

从S511
从S538
由分发信息数据库取得许可Key Kc
S540
根据Key KPcard(1)将Key Kc、数据License加密
S542
根据Key Ks1将[Kc, License]Kcard(1)加密
S544
发送[[Kc, License]Kcard(1)]Ks1
S546
根据Ks1解密
S550
将数据[Kc, License]Kcard(1)记录于存储器
S552
根据Kcard(1)将[Kc, License]Kcard(1)解密将数据License存放于寄存器
S554
将异常结束记录存放于管理数据库
S561
在销售机接收分发受理
S558
将销售记录存放于管理数据库
S560
结束
S562

图 43

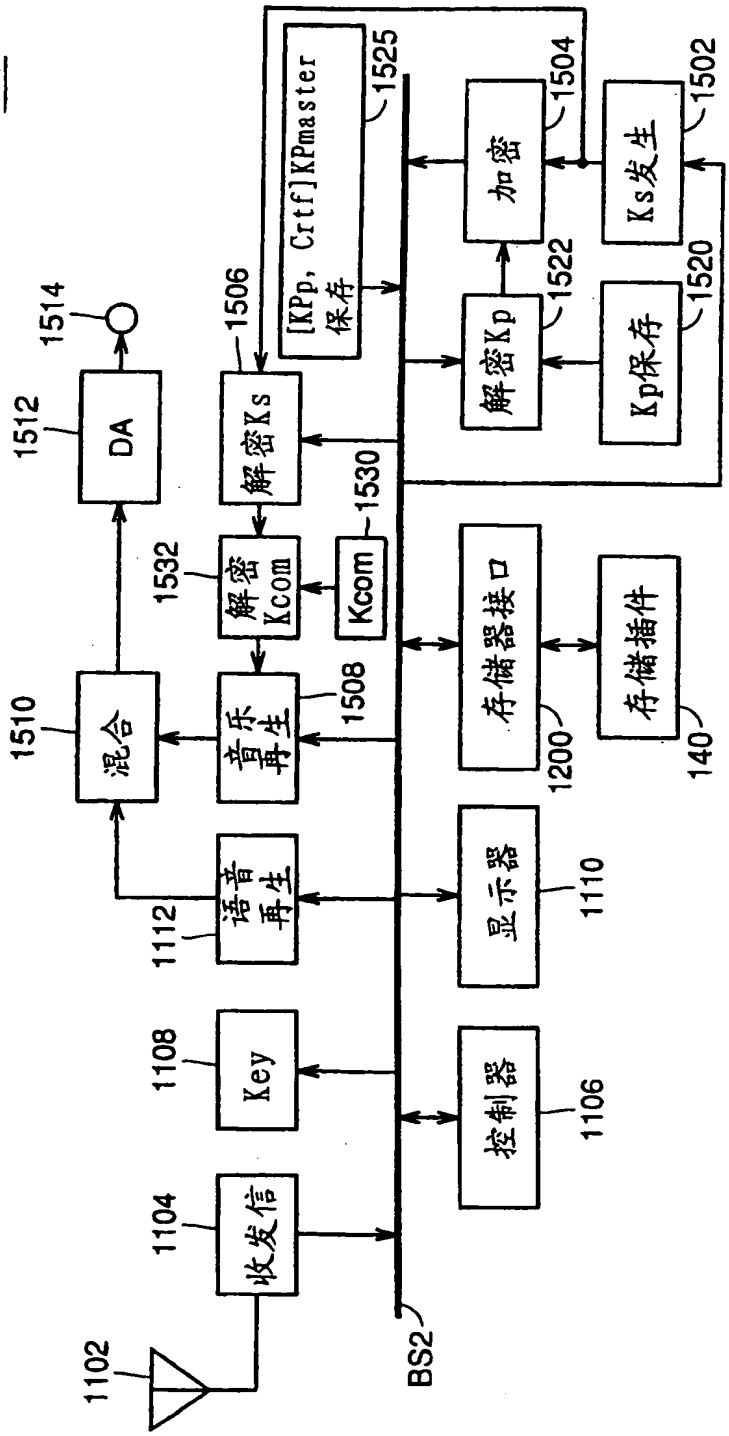

107
1102
1104
收发信
1108
Key
1112
话音再生
1510
混合
1512
DA
1514
1532
解密Kcom
1508
音乐再生
1530
Kcom
1506
解密Ks
[KPp, Crtf]KPmaster保存
1525
BS2
1106
控制器
1110
显示器
1200
存储器接口
140
存储插件
1504
加密
1522
解密Kp
1502
Ks发生
1520
Kp保存

图 44

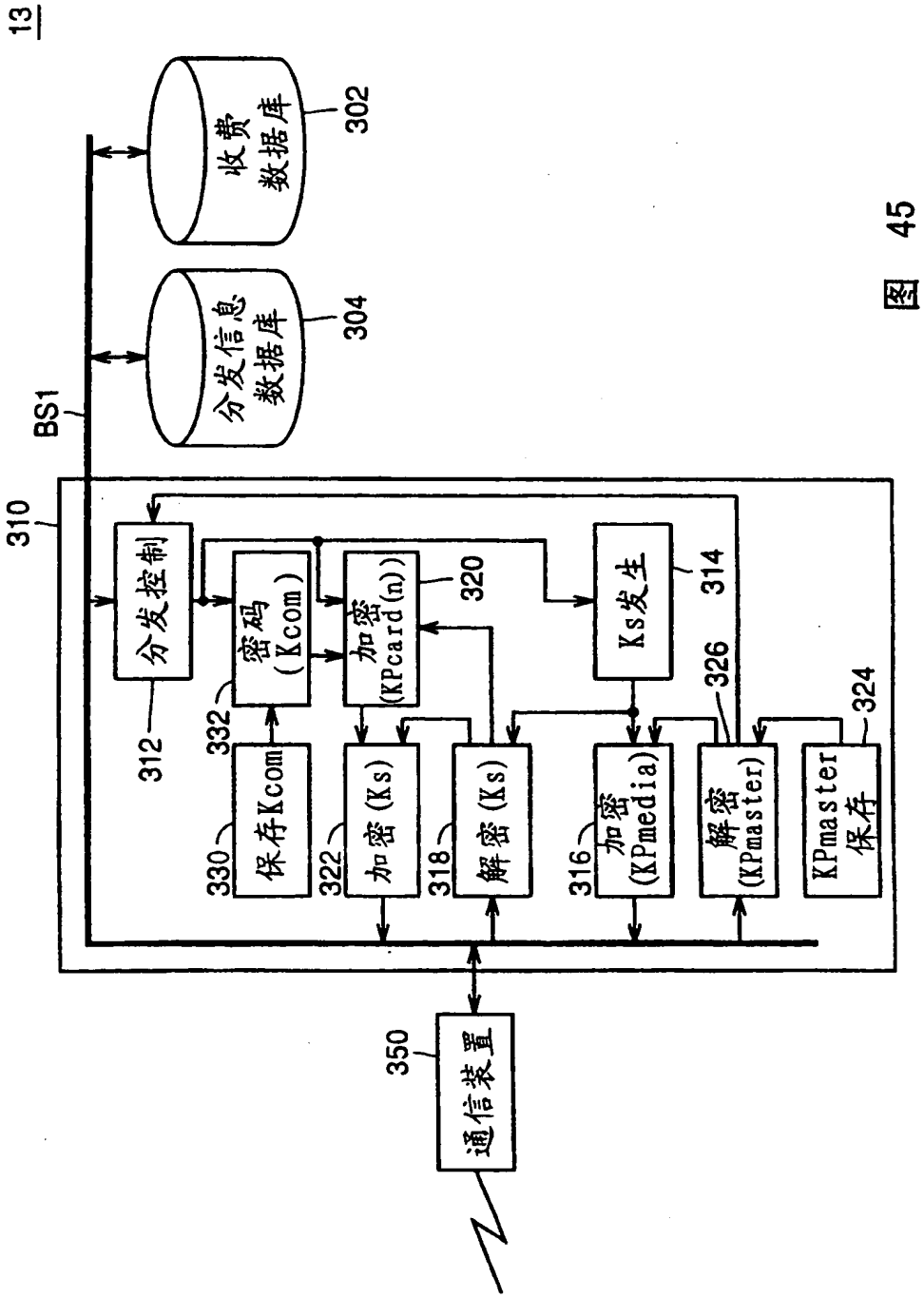

13
收费数据库
302
分发信息数据库
304
BS1
310
分发控制
312
密码(Kcom)
332
加密(KPcard(n))
320
Ks发生
314
保存Kcom
330
加密(Ks)
322
解密(Ks)
318
加密(KPmedia)
316
解密(KPmaster)
326
KPmaster保存
324
通信装置
350

图 45

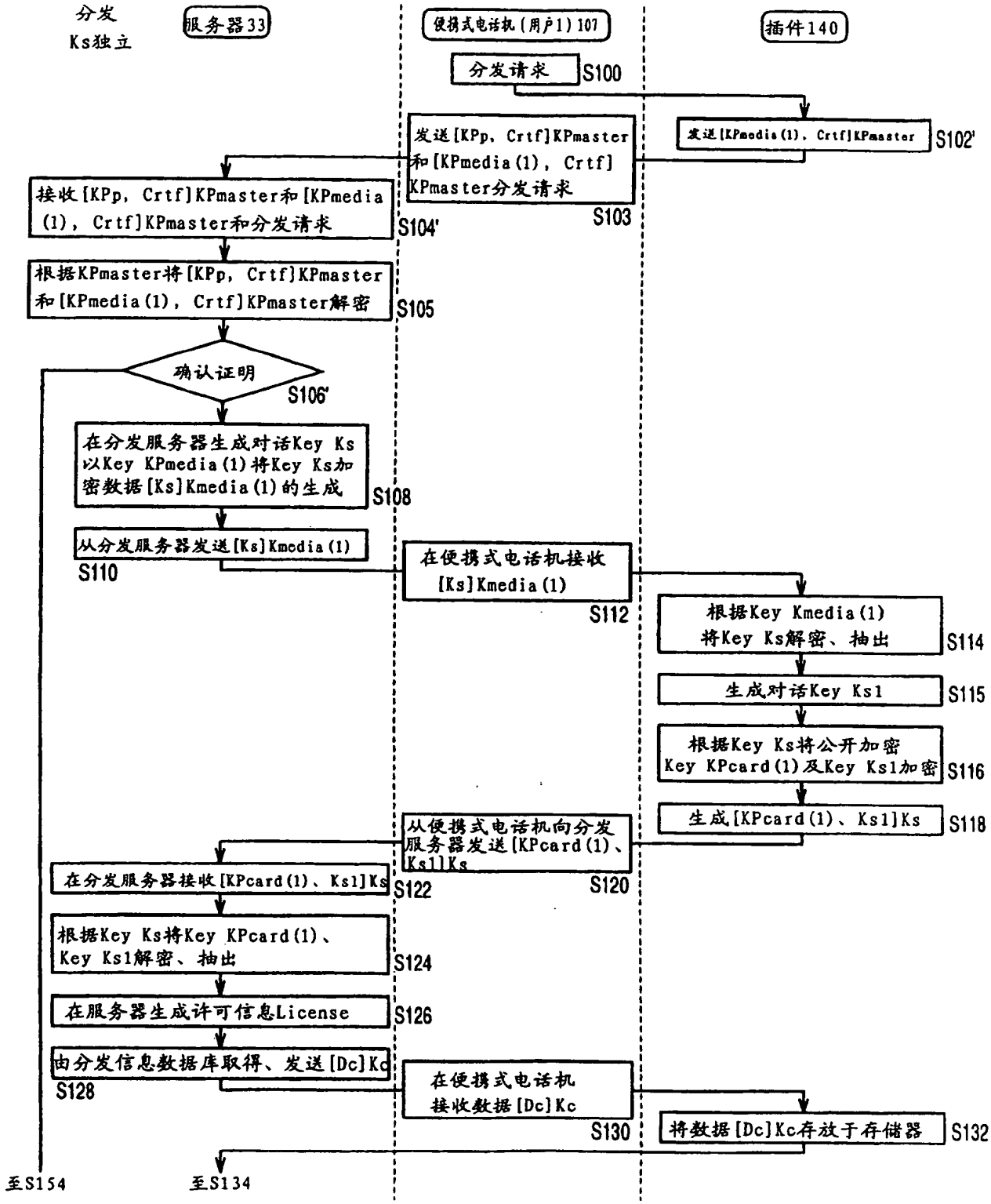

分发
Ks独立
服务器33
便携式电话机(用户1)107
插件140
分发请求
S100
发送[KPmedia(1), Crtf]KPmaster
S102'
发送[KPp, Crtf]KPmaster和[KPmedia(1), Crtf]KPmaster分发请求
S103
接收[KPp, Crtf]KPmaster和[KPmedia(1), Crtf]KPmaster和分发请求
S104'
根据KPmaster将[KPp, Crtf]KPmaster和[KPmedia(1), Crtf]KPmaster解密
S105
确认证明
S106'
在分发服务器生成对话Key Ks以Key KPmedia(1)将Key Ks加密数据[Ks]Kmedia(1)的生成
S108
从分发服务器发送[Ks]Kmedia(1)
S110
在便携式电话机接收[Ks]Kmedia(1)
S112
根据Key Kmedia(1)将Key Ks解密、抽出
S114
生成对话Key Ks1
S115
根据Key Ks将公开加密Key KPcard(1)及Key Ks1加密
S116
生成[KPcard(1)、Ks1]Ks
S118
从便携式电话机向分发服务器发送[KPcard(1)、Ks1]Ks
S120
在分发服务器接收[KPcard(1)、Ks1]Ks
S122
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S124
在服务器生成许可信息License
S126
由分发信息数据库取得、发送[Dc]Kc
S128
在便携式电话机接收数据[Dc]Kc
S130
将数据[Dc]Kc存放于存储器
S132
至S154
至S134

图 46

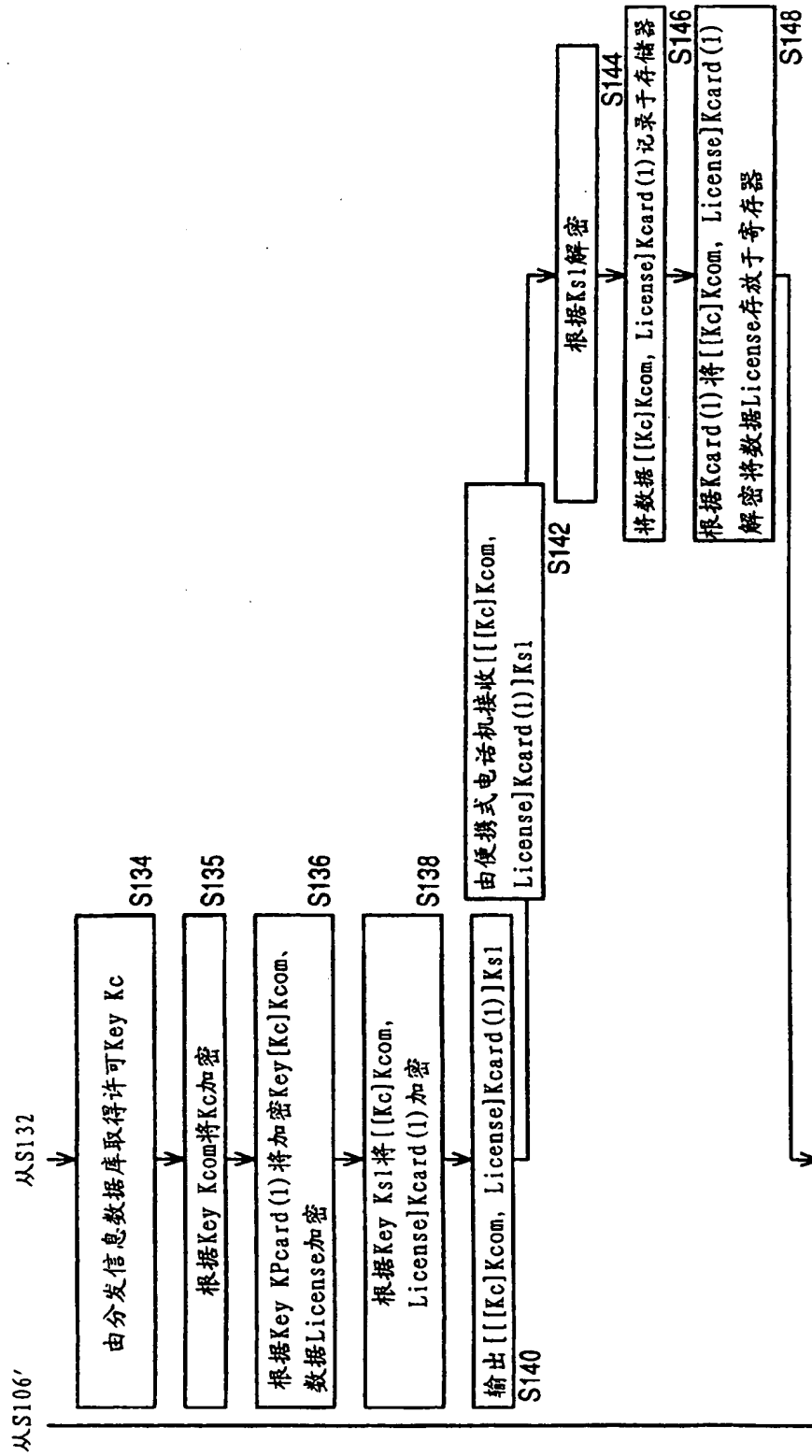

从S106'
从S132
由分发信息数据库取得许可Key Kc
S134
根据Key Kcom将Kc加密
S135
根据Key KPcard(1)将加密Key[Kc]Kcom、数据License加密
S136
根据Key Ks1将[[Kc]Kcom, License]Kcard(1)加密
S138
输出[[[Kc]Kcom, License]Kcard(1)]Ks1
S140
由便携式电话机接收[[[Kc]Kcom, License]Kcard(1)]Ks1
S142
根据Ks1解密
S144
将数据[[Kc]Kcom, License]Kcard(1)记录于存储器
S146
根据Kcard(1)将[[Kc]Kcom, License]Kcard(1)解密将数据License存放于寄存器
S148
在分发服务器接收分发受理
S150
记录于收费数据库
S152
结束
S154

图 47

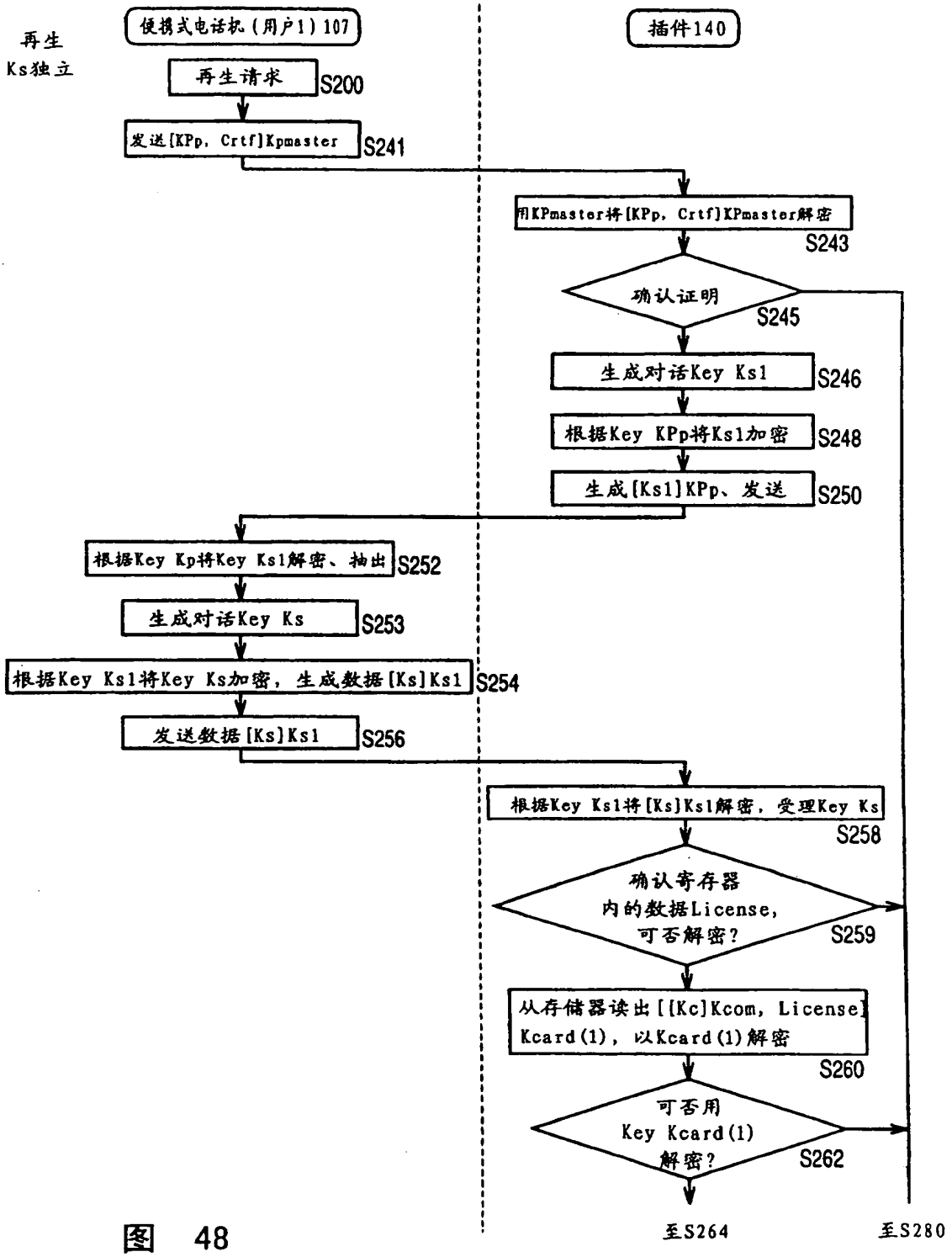

再生
Ks独立
便携式电话机（用户1）107
插件140
再生请求
S200
发送[KPp，Crtf]Kpmaster
S241
用KPmaster将[KPp，Crtf]KPmaster解密
S243
确认证明
S245
生成对话Key Ks1
S246
根据Key KPp将Ks1加密
S248
生成[Ks1]KPp、发送
S250
根据Key Kp将Key Ks1解密、抽出
S252
生成对话Key Ks
S253
根据Key Ks1将Key Ks加密，生成数据[Ks]Ks1
S254
发送数据[Ks]Ks1
S256
根据Key Ks1将[Ks]Ks1解密，受理Key Ks
S258
确认寄存器
内的数据License，
可否解密？
S259
从存储器读出[[Kc]Kcom，License]
Kcard(1)，以Kcard(1)解密
S260
可否用
Key Kcard(1)
解密？
S262
至S264
至S280

图 48

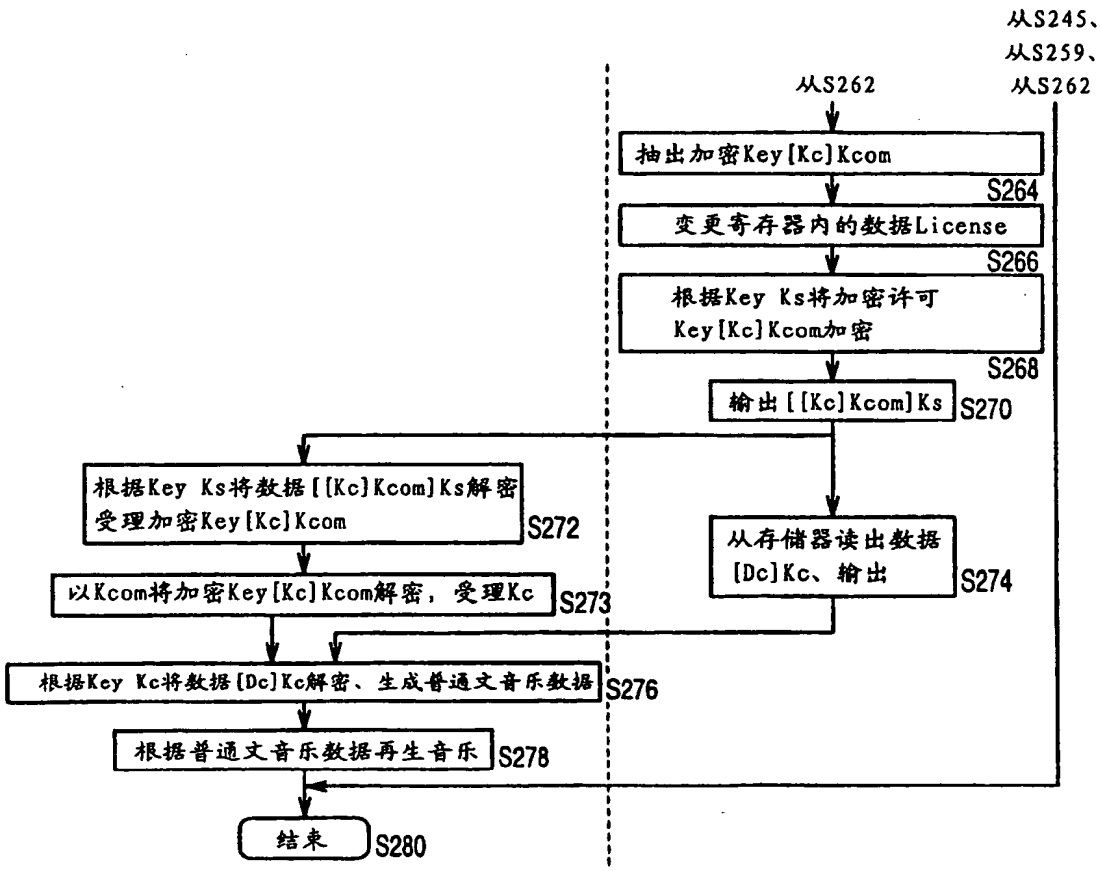

从S245、
从S259、
从S262
从S262
抽出加密Key[Kc]Kcom
S264
变更寄存器内的数据License
S266
根据Key Ks将加密许可
Key[Kc]Kcom加密
S268
输出[[Kc]Kcom]Ks
S270
根据Key Ks将数据[[Kc]Kcom]Ks解密
受理加密Key[Kc]Kcom
S272
从存储器读出数据
[Dc]Kc、输出
S274
以Kcom将加密Key[Kc]Kcom解密，受理Kc
S273
根据Key Kc将数据[Dc]Kc解密、生成普通文音乐数据
S276
根据普通文音乐数据再生音乐
S278
结束
S280

图 49

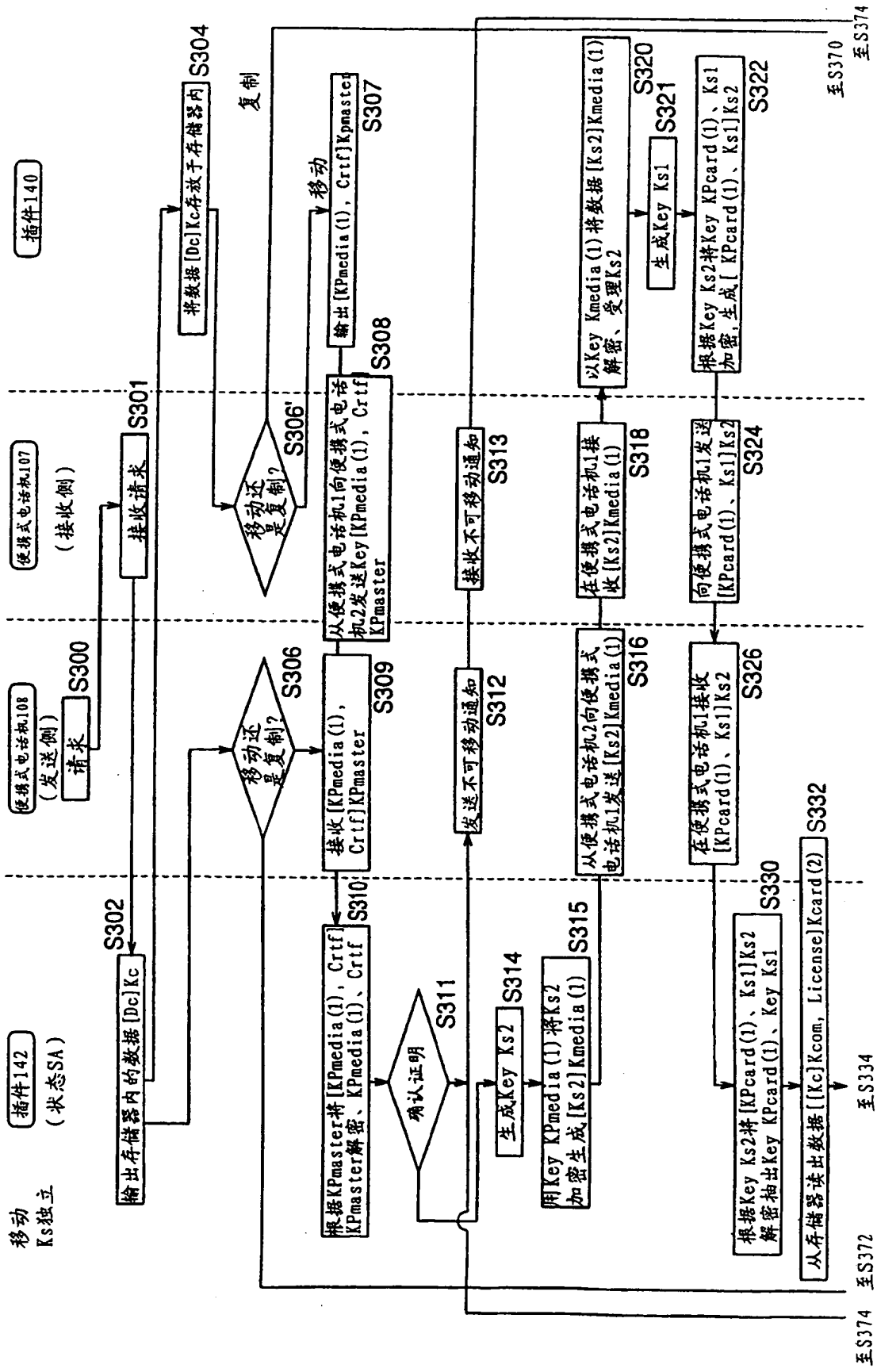

移动
Ks独立
插件142
(状态SA)
便携式电话机108
(发送侧)
请求
S300
插件140
便携式电话机107
(接收侧)
接收请求
S301
输出存储器内的数据[Dc]Kc
S302
将数据[Dc]Kc存放于存储器内
S304
复制
移动还是复制?
S306'
移动
输出[KPmedia(1), Crtf]Kpmaster
S307
从便携式电话机1向便携式电话机2发送Key[KPmedia(1), Crtf]KPmaster
S308
移动还是复制?
S306
接收[KPmedia(1), Crtf]KPmaster
S309
根据KPmaster将[KPmedia(1), Crtf]KPmaster解密、KPmedia(1)、Crtf
S310
确认证明
S311
发送不可移动通知
S312
接收不可移动通知
S313
生成Key Ks2
S314
用Key KPmedia(1)将Ks2加密生成[Ks2]Kmedia(1)
S315
从便携式电话机2向便携式电话机1发送[Ks2]Kmedia(1)
S316
在便携式电话机1接收[Ks2]Kmedia(1)
S318
以Key Kmedia(1)将数据[Ks2]Kmedia(1)解密、受理Ks2
S320
生成Key Ks1
S321
根据Key Ks2将Key KPcard(1)、Ks1加密,生成[KPcard(1)、Ks1]Ks2
S322
向便携式电话机1发送[KPcard(1)、Ks1]Ks2
S324
在便携式电话机1接收[KPcard(1)、Ks1]Ks2
S326
根据Key Ks2将[KPcard(1)、Ks1]Ks2解密抽出Key KPcard(1)、Key Ks1
S330
从存储器读出数据[[Kc]Kcom, License]Kcard(2)
S332
至S372
至S334
至S374
至S370
至S374

图 50

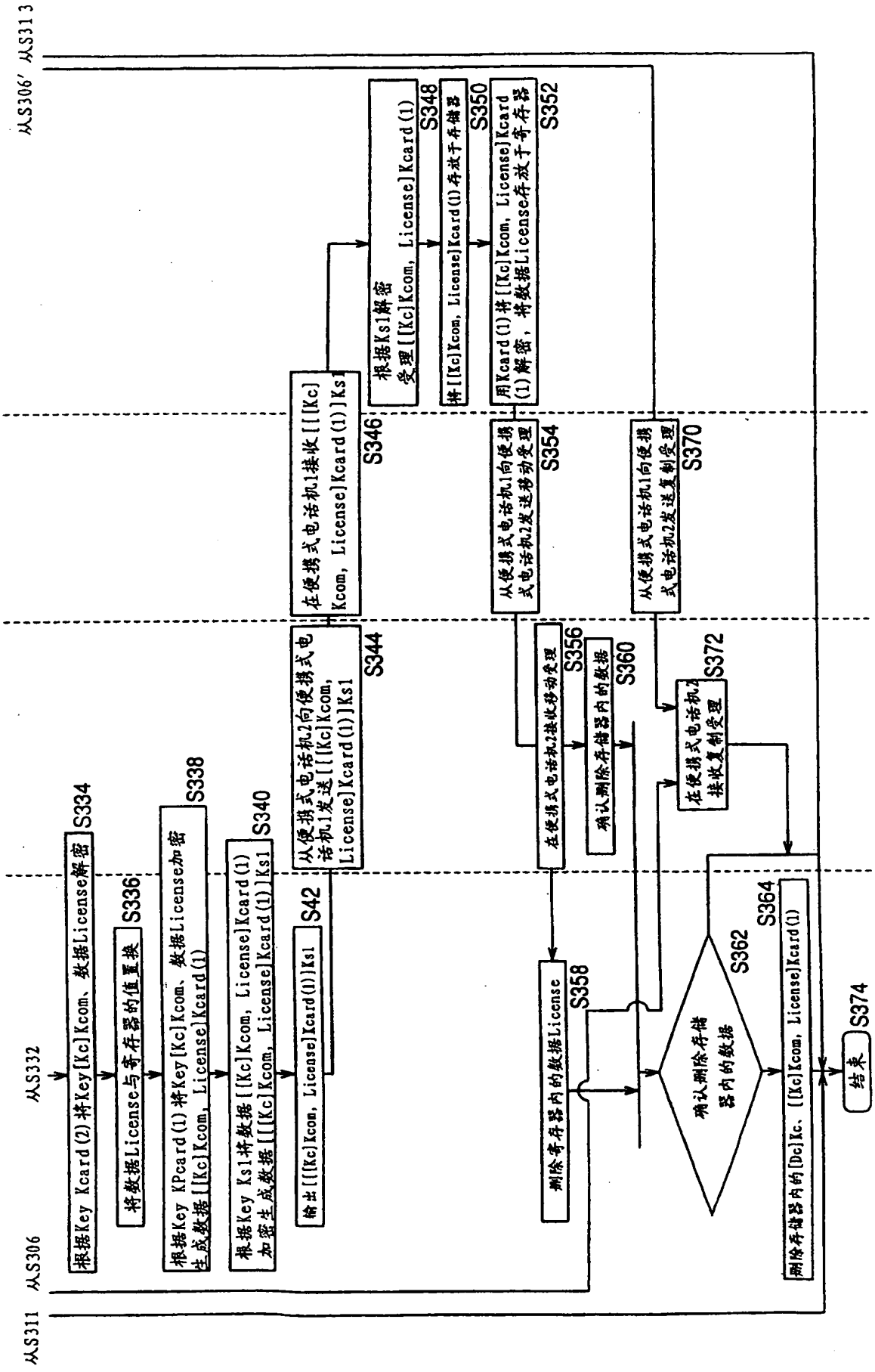

从S311
从S306
根据Key Kcard(2)将Key[Kc]Kcom、数据License解密
S334
将数据License与寄存器的值置换
S336
根据Key KPcard(1)将Key[Kc]Kcom、数据License加密生成数据[[Kc]Kcom, License]Kcard(1)
S338
根据Key Ks1将数据[[Kc]Kcom, License]Kcard(1)加密生成数据[[[Kc]Kcom, License]Kcard(1)]Ks1
S340
输出[[[Kc]Kcom, License]Kcard(1)]Ks1
S42
从S332
从便携式电话机2向便携式电话机1发送[[[Kc]Kcom, License]Kcard(1)]Ks1
S344
在便携式电话机1接收[[[Kc]Kcom, License]Kcard(1)]Ks1
S346
从S306′ 从S313
根据Ks1解密受理[[Kc]Kcom, License]Kcard(1)
S348
将[[Kc]Kcom, License]Kcard(1)存放于寄存器
S350
用Kcard(1)将[[Kc]Kcom, License]Kcard(1)解密，将数据License存放于寄存器
S352
从便携式电话机1向便携式电话机2发送移动受理
S354
从便携式电话机1向便携式电话机2发送复制受理
S370
在便携式电话机2接收移动受理
S356
确认删除存储器内的数据
S360
在便携式电话机2接收复制受理
S372
删除寄存器内的数据License
S358
确认删除存储器内的数据
S362
删除存储器内的[Dc]Kc、[[Kc]Kcom, License]Kcard(1)
S364
结束
S374

图 51

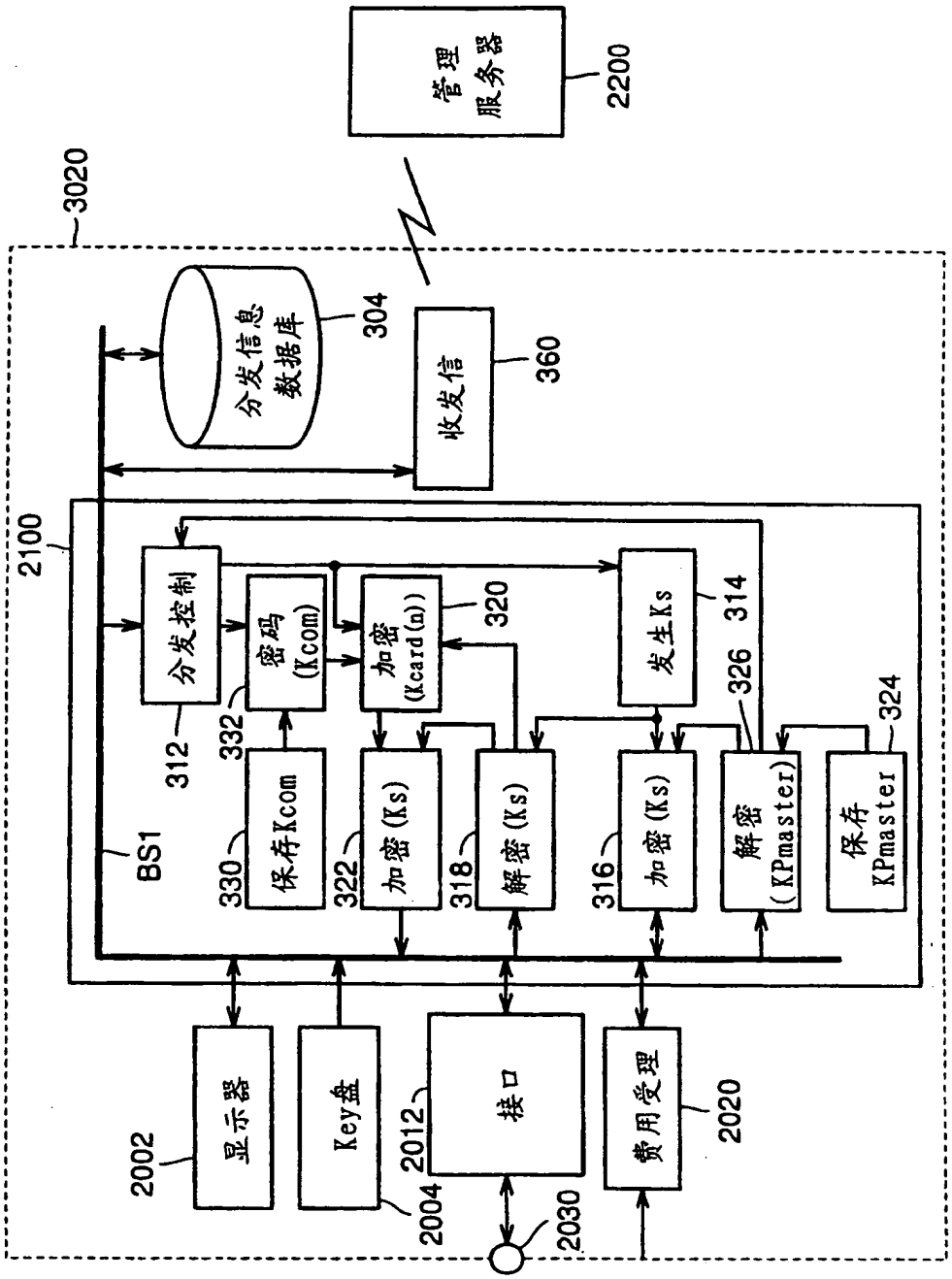

管理服务器
2200
3020
分发信息数据库
304
收发信
360
2100
分发控制
312
密码(Kcom)
332
加密(Kcard(n))
320
发生Ks
314
326
324
BS1
保存Kcom
330
加密(Ks)
322
解密(Ks)
318
加密(Ks)
316
解密(KPmaster)
保存KPmaster
显示器
2002
Key盘
2004
接口
2012
2030
费用受理
2020

图 52

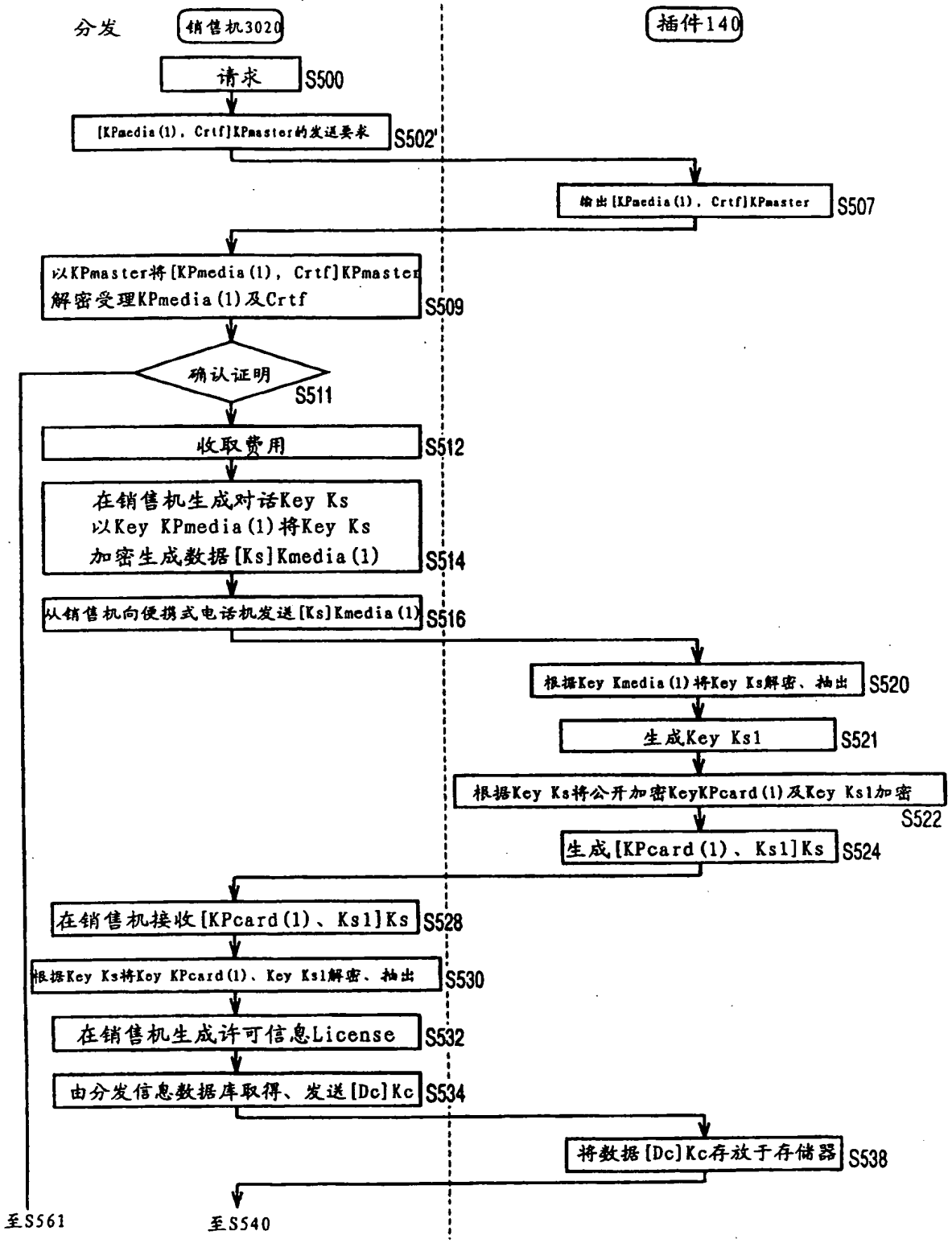

分发
销售机3020
插件140
请求
S500
[KPmedia(1), Crtf]KPmaster的发送要求
S502'
输出[KPmedia(1), Crtf]KPmaster
S507
以KPmaster将[KPmedia(1), Crtf]KPmaster
解密受理KPmedia(1)及Crtf
S509
确认证明
S511
收取费用
S512
在销售机生成对话Key Ks
以Key KPmedia(1)将Key Ks
加密生成数据[Ks]Kmedia(1)
S514
从销售机向便携式电话机发送[Ks]Kmedia(1)
S516
根据Key Kmedia(1)将Key Ks解密、抽出
S520
生成Key Ks1
S521
根据Key Ks将公开加密KeyKPcard(1)及Key Ks1加密
S522
生成[KPcard(1)、Ks1]Ks
S524
在销售机接收[KPcard(1)、Ks1]Ks
S528
根据Key Ks将Key KPcard(1)、Key Ks1解密、抽出
S530
在销售机生成许可信息License
S532
由分发信息数据库取得、发送[Dc]Kc
S534
将数据[Dc]Kc存放于存储器
S538
至S561
至S540

图 53

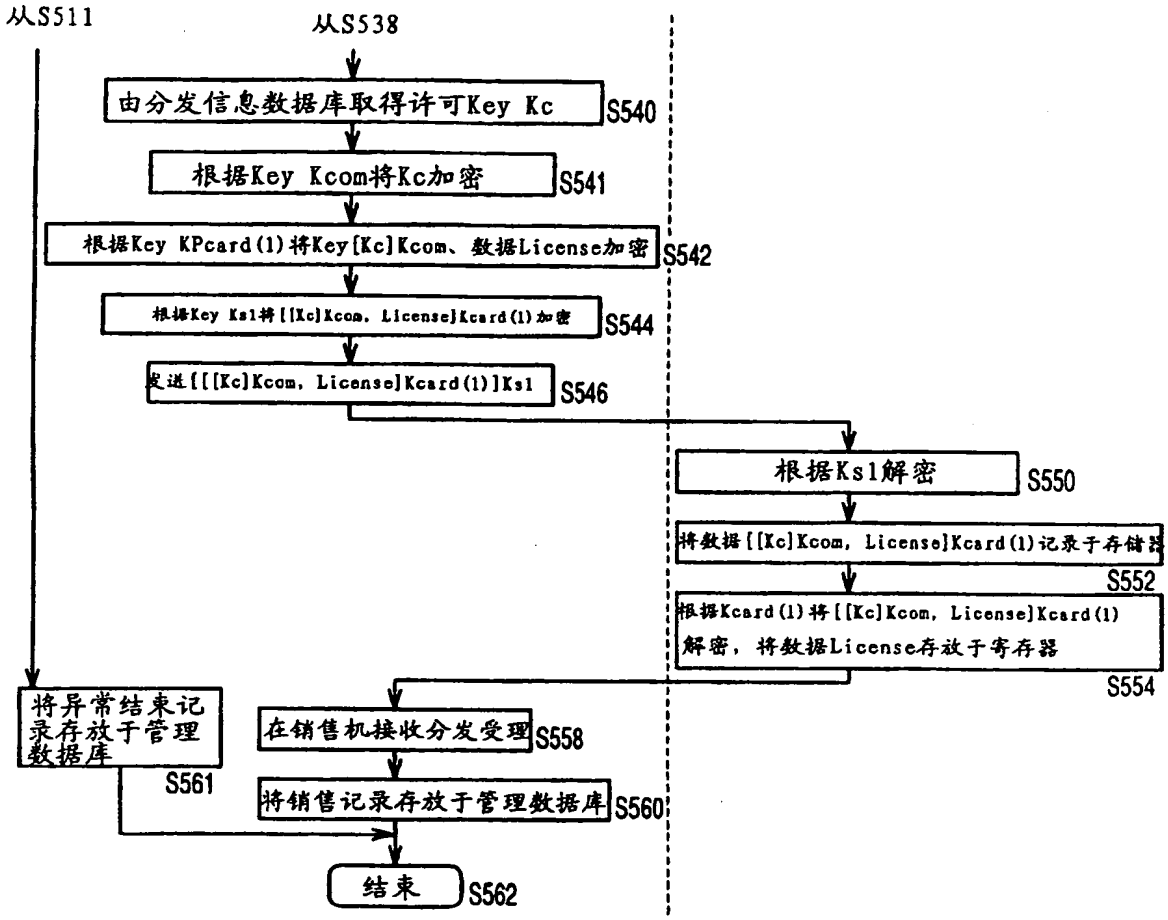

从S511
从S538
由分发信息数据库取得许可Key Kc
S540
根据Key Kcom将Kc加密
S541
根据Key KPcard(1)将Key[Kc]Kcom、数据License加密
S542
根据Key Ks1将[[Kc]Kcom, License]Kcard(1)加密
S544
发送[[[Kc]Kcom, License]Kcard(1)]Ks1
S546
根据Ks1解密
S550
将数据[[Kc]Kcom, License]Kcard(1)记录于存储器
S552
根据Kcard(1)将[[Kc]Kcom, License]Kcard(1)
解密，将数据License存放于寄存器
S554
将异常结束记录存放于管理数据库
S561
在销售机接收分发受理
S558
将销售记录存放于管理数据库
S560
结束
S562

图 54

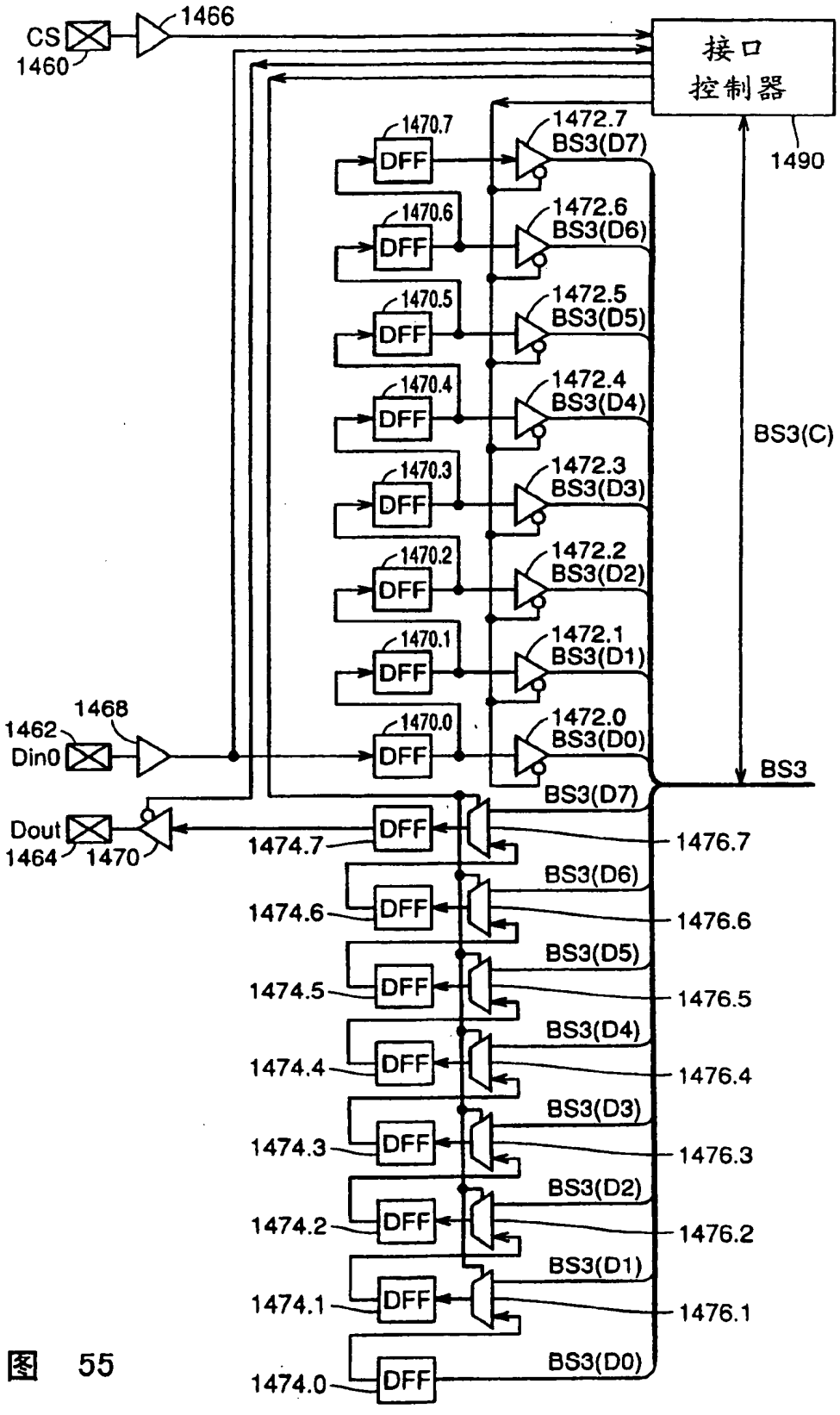

CS
1460
1466
接口
控制器
1490
1470.7
DFF
1472.7
BS3(D7)
1470.6
DFF
1472.6
BS3(D6)
1470.5
DFF
1472.5
BS3(D5)
1470.4
DFF
1472.4
BS3(D4)
BS3(C)
1470.3
DFF
1472.3
BS3(D3)
1470.2
DFF
1472.2
BS3(D2)
1470.1
DFF
1472.1
BS3(D1)
1468
1462
Din0
1470.0
DFF
1472.0
BS3(D0)
BS3
BS3(D7)
Dout
1464
1470
1474.7
DFF
1476.7
BS3(D6)
1474.6
DFF
1476.6
BS3(D5)
1474.5
DFF
1476.5
BS3(D4)
1474.4
DFF
1476.4
BS3(D3)
1474.3
DFF
1476.3
BS3(D2)
1474.2
DFF
1476.2
BS3(D1)
1474.1
DFF
1476.1
BS3(D0)
1474.0
DFF

图 55

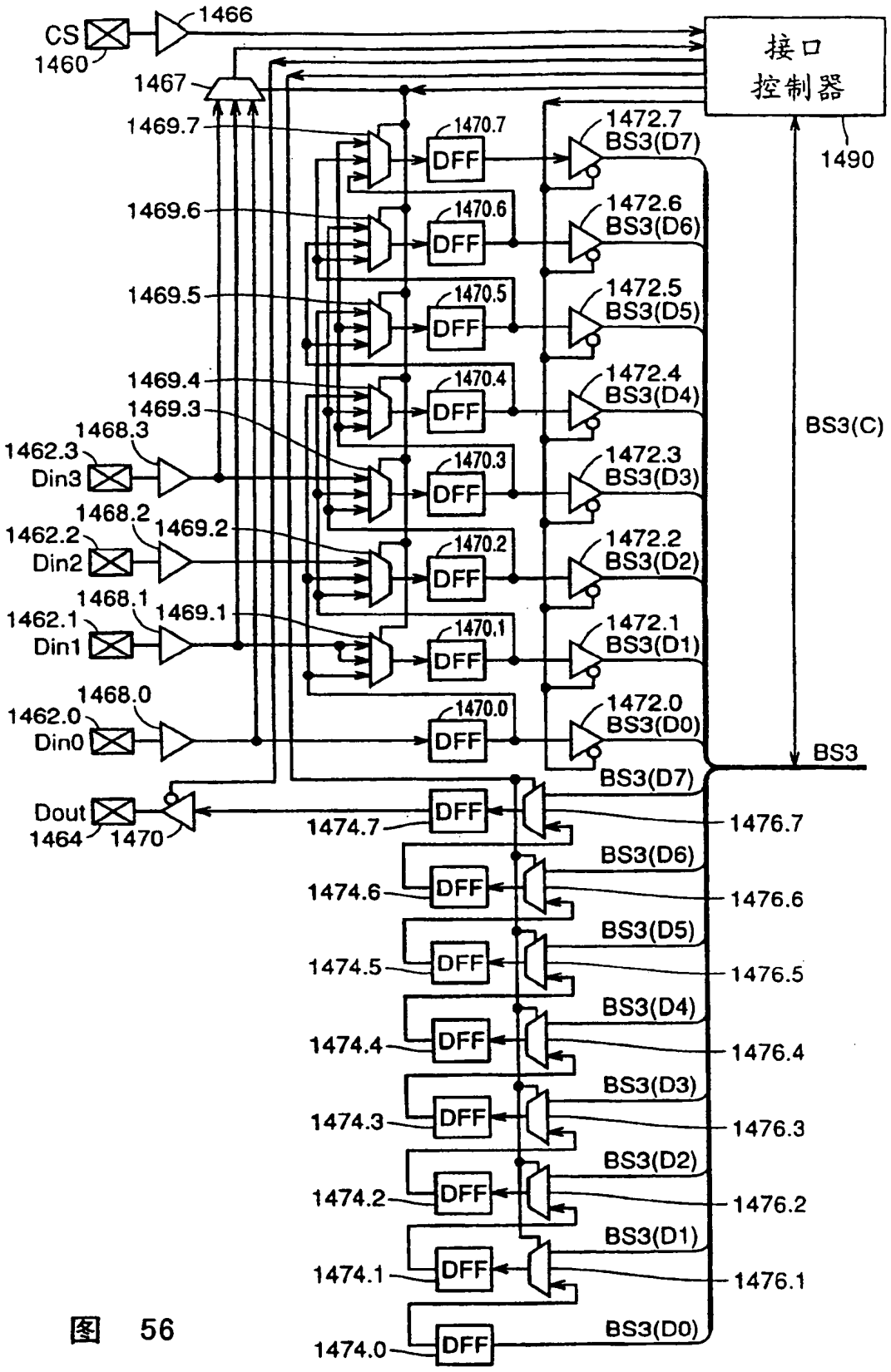

CS
1460
1466
1467
接口
控制器
1490
1469.7
1469.6
1469.5
1469.4
1469.3
1469.2
1469.1
1468.3
1462.3
Din3
1468.2
1462.2
Din2
1468.1
1462.1
Din1
1468.0
1462.0
Din0
Dout
1464
1470
DFF
1470.7
1470.6
1470.5
1470.4
1470.3
1470.2
1470.1
1470.0
1472.7
BS3(D7)
1472.6
BS3(D6)
1472.5
BS3(D5)
1472.4
BS3(D4)
1472.3
BS3(D3)
1472.2
BS3(D2)
1472.1
BS3(D1)
1472.0
BS3(D0)
BS3(C)
BS3
1474.7
1474.6
1474.5
1474.4
1474.3
1474.2
1474.1
1474.0
1476.7
1476.6
1476.5
1476.4
1476.3
1476.2
1476.1

图 56